BRUCE E. MESERVE

Conceptos fundamentales de álgebra

Ediciones de la
UNIVERSIDAD DE CHILE

Conceptos fundamentales de álgebra

CONCEPTOS FUNDAMENTALES DE ALGEBRA
por *Bruce E. Meserve*

Título original: *Fundamental Concepts of Algebra*

Versión castellana publicada por convenio entre la
Universidad de Chile y Addison-Wesley Publishing Company, Inc., EE. UU.

Traducción de *Amalia Villarroel,*
Profesora de Estado.

Obra editada por acuerdo de la
COMISION CENTRAL DE PUBLICACIONES
DE LA UNIVERSIDAD DE CHILE

Edición al cuidado del profesor *Félix Schwartzmann.*

© 1953, Addison-Wesley Publishing Company, Inc., EE. UU.
© de la traducción castellana: Ediciones de la Universidad de Chile. 1965.
Inscripción en el Registro de la Propiedad Intelectual Nº 34.460.
Library of Congress Catalog Nº 52-12052.

Composición: Linotype Baskerville 10/12.
Papel: Hilado especial de la Cía. Manufacturera de Papeles y Cartones.
Impreso en los talleres de la EDITORIAL UNIVERSITARIA, S. A.
San Francisco 454. Santiago, Chile.

Proyectó la edición *Mauricio Amster.*
Portada de *Hernán Valdés.*
PRINTED IN CHILE

BRUCE E. MESERVE

Conceptos fundamentales de álgebra

Traducción de AMALIA VILLARROEL

Ediciones de la
UNIVERSIDAD DE CHILE
Santiago de Chile, 1968

Indice

Nota preliminar de la traductora 9
Prólogo 12

Capítulo I. NUESTRO SISTEMA DE NÚMEROS

I-1 Conjuntos 13
I-2 Los números cardinales . . 15
I-3 Relaciones de equivalencia . 20
I-4 Los postulados de Peano . . 22
I-5 La adición y la multiplicación 24
I-6 Relaciones de orden . . . 29
I-7 Números inversos y operaciones inversas 31
I-8 Los números racionales positivos 33
I-9 Los números negativos . . 37
I-10 Los números reales . . . 42
I-11 Los postulados de los números reales 46
I-12 Propiedades de los números reales 50
I-13 Los números cardinales transfinitos 56
I-14 Grupo: sistema de números . 60
I-15 Los números complejos . . 63
I-16 Propiedades de los números complejos 69
I-17 Teorema de De Moivre . . 74
I-18 Campos y sistemas de números 79

Capítulo II. TEORÍA DE LOS NÚMEROS

II-1 Divisibilidad 86
II-2 El algoritmo de la división . 88
II-3 Números primos 91
II-4 Teorema de la factorización única 96
II-5 El algoritmo de Euclides . 101
II-6 Bases 106
II-7 Notación decimal 113
II-8 Congruencias 116
II-9 Clases residuales. Función ϕ de Euler 120
II-10 Evaluación de ϕ (m) . . . 124
II-11 Congruencias lineales . . . 127
II-12 Problemas diofánticos . . 131

Capítulo III. TEORÍA DE LOS POLINOMIOS

III-1 Polinomios 135
III-2 Anillos de polinomios . . . 137
III-3 Funciones racionales . . . 139
III-4 Divisibilidad 140
III-5 El algoritmo de la división . 142
III-6 Polinomios irreducibles . . 145
III-7 El algoritmo de Euclides . 148
III-8 Cambio de variable . . . 151
III-9 Ideales 153
III-10 Funciones 154
III-11 Límites 158
III-12 Continuidad 163
III-13 Funciones continuas . . . 166
III-14 Derivadas 170
III-15 Serie de Taylor 173
III-16 Funciones analíticas . . . 175

Capítulo IV. TEORÍA DE LAS ECUACIONES

IV-1 Ceros de un polinomio . . 178
IV-2 División sintética 179
IV-3 Cambio de variable . . . 181
IV-4 Número de raíces 183
IV-5 Determinación de las raíces 185
IV-6 Raíces imaginarias conjugadas 187
IV-7 Polinomios elementales simétricos 188
IV-8 Transformaciones de raíces . 191
IV-9 Ecuaciones cúbicas . . . 196
IV-10 Ecuaciones de cuarto grado . 200
IV-11 La regla de Descartes para los signos 202
IV-12 Teorema de Sturn 207
IV-13 Raíces múltiples 212
IV-14 Soluciones aproximadas . . 217

Capítulo V. DETERMINANTES Y MATRICES

v-1 Desarrollo histórico . . . 221
v-2 Matrices 223
v-3 Permutaciones 225
v-4 Inversiones 227
v-5 Transposiciones 229
v-6 Permutaciones pares e impares 232
v-7 Determinantes 234
v-8 Propiedades de los determinantes 239
v-9 Desarrollo de los determinantes 245
v-10 Determinantes menores . . 252
v-11 Regla de Cramer 260
v-12 Sistemas de ecuaciones lineales 264
v-13 Dependencia lineal 268
v-14 Aplicaciones en geometría analítica 275
v-15 Transformaciones geométricas 279

Capítulo VI. CONSTRUCCIONES

vi-1 Construcciones clásicas . . 289
vi-2 Construcciones clásicas elementales 290
vi-3 El punto de vista algebraico 292
vi-4 Construcciones clásicas básicas 293
vi-5 Construcciones de raíces de ecuaciones 296
vi-6 Problemas de construcción famosos 299
vi-7 Trisecciones geométricas no clásicas 303
vi-8 Trisectores de ángulo mecánicos 306
vi-9 Polígonos articulados . . . 308
vi-10 Resumen 310

Capítulo VII. REPRESENTACIONES GRÁFICAS

vii-1 Los espacios euclidiano y complejo 313
vii-2 Polinomios 315
vii-3 Secciones cónicas 218
vii-4 Superficies cuádricas . . . 323
vii-5 Curvas planas de grado superior 327
vii-6 Funciones racionales . . . 329
vii-7 Funciones algebraicas . . . 334
vii-8 Trazado de curvas 336
vii-9 Gráficos especiales 241
vii-10 Soluciones gráficas 343
vii-11 Determinación de curvas . . 345
vii-12 Conclusión 349

Bibliografía 351
Indice alfabético 355
Símbolos y notas 363

Nota preliminar de la traductora

Para iniciar en el estudio del álgebra a los alumnos universitarios, existen numerosos textos —tanto en castellano como en otros idiomas— que presentan las materias en forma sistemática. Pero el texto escrito por el profesor Bruce E. Meserve difiere notablemente de esas obras, porque elude el tratamiento sistemático del análisis algebraico y presenta aquellos conceptos fundamentales que confieren unidad a la matemática y que por ser tan generales, se encuentran en todas las ramas de esta ciencia.

Pocos textos de matemática tienen el atractivo que posee este libro, cuyo acierto principal es, sin lugar a dudas, la nueva orientación que da a las materias, al presentar el estudio de los temas del álgebra clásica desde el punto de vista del álgebra moderna, en forma tan general, que ésta sirve de enlace entre las dos posiciones.

El lenguaje sencillo y claro —reflejo, sin duda, del empleado por el autor en sus largos años de docencia—, contribuye a prestarle ese atractivo, al mismo tiempo que realza su valor didáctico. La traductora se ha esforzado por conservar estas cualidades en la versión castellana.

AMALIA VILLARROEL BASCOPÉ

Prólogo

El presente libro se basa sobre un curso de álgebra, que forma parte de aquél que bajo el título de "Conceptos fundamentales de matemáticas" se ha estado desarrollando en la Universidad de Illinois en el transcurso de los últimos cuarenta años. En él se presentan y se aplican los temas de análisis junto con los de álgebra. El curso en referencia se completa con otro volumen dedicado principalmente a conceptos fundamentales de geometría.

Se ha adoptado aquí un punto de vista moderno del álgebra y del análisis, es decir, se reconoce la necesidad básica de conocer los conceptos fundamentales de estas materias, fuera de lo que proporcionan los cursos especializados de cada una de sus muchas subdivisiones. Dicha necesidad la experimentan sobre todo los futuros profesores de matemáticas de nivel secundario, los estudiantes de nivel pre-universitario que se preparan para cursos superiores especializados de matemáticas y cualquiera persona que desee una amplia educación liberal.

Durante varios años el autor y otros han empleado como texto la versión mimeografiada de este libro en el nivel superior preuniversitario y en los cursos de graduados*. La mayoría de los estudiantes de este nivel han estudiado, previamente, matemáticas (*college mathematics*) hasta el cálculo. Sin embargo, este libro también se ha empleado con éxito en aquellos casos en que no se exigía el cálculo como requisito previo. Hay abundante material para un curso de cuarenta y cinco horas de clase.

*El texto dice "advanced undergraduate-graduate level". (N. de la T.).

Al tratar el sistema de números complejos y las teorías elementales de números, polinomios y ecuaciones (Cap. I a IV) se aplican los conceptos y la terminología del álgebra moderna. Los Capítulos V (Determinantes y Matrices) y VI (Construcciones) dependen de los primeros cuatro capítulos, pero son independientes entre sí. El vasto alcance de este libro se debe a que se han considerado principalmente los conceptos fundamentales dentro de las diversas materias. Estos conceptos se ilustran con numerosos ejemplos y frecuentemente la teoría se amplía mediante series adecuadas de ejercicios. Este libro se preocupa principalmente de los conceptos fundamentales de las matemáticas superiores (álgebra y análisis) en su relación con las matemáticas elementales. De esta manera, pretende introducir los conceptos de las matemáticas superiores y lograr así que el lector adquiera un conocimiento acabado de las matemáticas elementales.

El autor expresa sus agradecimientos al profesor E. B. Lytle, al profesor Echo Pepper y a la profesora J. H. Chanler, por su contribución al desarrollo del curso que dio origen a este libro. Cabe agregar que la profesora Chanler ha empleado como texto, en sus clases, la versión mimeografiada de este libro e hizo muchas sugerencias valiosas durante toda la preparación del manuscrito.

También debo agradecer las críticas constructivas de muchos alumnos, al profesor F. E. Hohn, que leyó el manuscrito, a mi esposa, que dactilografió el manuscrito, y a los editores por su cooperación y su eficiente desempeño. El autor está sinceramente agradecido de todos y de cada uno de ellos.

BRUCE E. MESERVE

Diciembre, 1952.

CAPITULO 1

Nuestro sistema de números

Casi todo el mundo emplea diariamente un sistema de números, sin embargo, pocos pueden describir con exactitud lo que es un sistema de números. En este capítulo nos esforzaremos por conseguir una apreciación correcta de lo que son los números y algunas de sus relaciones entre ellos. A continuación se presenta un método de estudio de los tres sistemas de números que se usan más corrientemente hoy día: los números racionales, los números reales y los números complejos. Durante este estudio resultará evidente que estos tres sistemas se relacionan de modo que los números reales comprenden a los números racionales, y los complejos comprenden a los reales y a los racionales. Se mencionarán, brevemente, algunos otros sistemas de números.

I-1 CONJUNTOS. Los números se asocian frecuentemente a conjuntos de objetos. Tres hombres, tres piedras, tres troncos, tienen una propiedad común que pudo haberse indicado primitivamente por ///. Presentaremos unas cuantas propiedades de los números en términos de conjuntos (se definen oportunamente) y de correspondencias entre conjuntos. Más adelante, adoptaremos algunos postulados como base para un estudio más completo de los números.

El concepto de conjunto, clase, colección de elementos es fundamental, no solamente en matemáticas, sino también en la vida diaria. Por ejemplo, uno a menudo se refiere a un par de zapatos, a un juego de palos de golf, a un juego de piezas de ajedrez, a una

baraja de naipes, a una colección de libros, a un juego de neumáticos para un automóvil, etc. En matemáticas se podría considerar el conjunto de números enteros positivos, los tres vértices de un triángulo, las raíces de una ecuación polinomia, el conjunto de números enteros positivos pares menores que 1.000, el conjunto de números primos positivos, la totalidad de los números reales, etc. En rigor, parafraseando a G. Cantor, definiremos un *conjunto** *S* como la reunión en un todo de objetos percibidos o considerados distintos; estos objetos se denominan los *elementos* de *S*. En la práctica, el lector logrará comprender todo el significado e importancia de este concepto (así como de muchos otros), a medida que se haga mayor uso de él.

Los números que el hombre primitivo usó primero para contar los elementos de un conjunto de objetos se llaman *números naturales* o *números enteros positivos.* Técnicamente, los números enteros positivos son símbolos. Pueden escribirse como /, //, ///, ...; i, ii, iii, ...; 1, 2, 3, ...; o de muchas otras maneras. Existen también muchos otros símbolos, tales como 0, -3, $\sqrt{2}$, y π, que más adelante definiremos como números; es decir, ampliaremos el significado de "número" para incluir símbolos que no son enteros positivos. Sin embargo, consideraremos primero algunas de las propiedades básicas de los números enteros positivos.

Cuando los enteros positivos se usan para contar los elementos de un conjunto, suelen llamarse *números ordinales;* cuando se emplean para designar el número de elementos de un conjunto, se llaman *números cardinales.* Consideraremos el concepto de número cardinal en términos de las propiedades comunes de los conjuntos, de cualquier clase de conjuntos que tengan el mismo número cardinal.

La propiedad común a los conjuntos de tres hombres, tres piedras, tres troncos, pudo haberse observado por primera vez cuando cada hombre tenía una piedra en su mano o estaba sentado en un tronco. Esta propiedad común se comprende más fácilmente si se expresa por medio de correspondencias biunívocas, otro concepto fundamental de las matemáticas. Existe una *correspondencia biunívoca* entre los elementos de los conjuntos A y B, siempre que cada elemento del conjunto A corresponda exactamente

*En el presente texto se indicarán con letra cursiva los términos nuevos al ser definidos o identificados por primera vez.

a un elemento del conjunto B y cada elemento del conjunto B sea el correspondiente de exactamente un elemento del conjunto A. El número cardinal b de cualquier conjunto B, designa una propiedad común de todos los conjuntos A_a tales que los elementos de cada conjunto A_a puedan coordinarse en correspondencia biunívoca con los elementos de B.

Podemos asociar, el mismo número 3, con cada uno de los conjuntos de hombres, de piedras y de troncos si y sólo si podemos contar los elementos de cada conjunto empleando los enteros 1, 2, 3, es decir, si existe correspondencia biunívoca entre cada conjunto y el conjunto de los enteros positivos 1, 2, 3. De aquí que el número 3 represente una propiedad común a los conjuntos de tres enteros, tres hombres, tres piedras, tres troncos y a cualquier otro conjunto de elementos que puedan coordinarse en correspondencia biunívoca con cualquiera de estos conjuntos. En otras palabras, todos los conjuntos que pueden coordinarse en correspondencia biunívoca con el conjunto 1, 2, 3, tienen una propiedad común que se designa con el número cardinal 3. En este sentido, el número cardinal 3 sirve para denotar cualquier conjunto de esta clase de conjuntos. Este concepto y el concepto de correspondencia biunívoca entre conjuntos, constituye el fundamento de nuestro estudio sobre las propiedades de los números cardinales.

EJERCICIOS

1. Nombrar o describir dos conjuntos de elementos que tengan el número cardinal 4 e indicar cómo se puede establecer entre ellos una correspondencia biunívoca.
2. Repetir el Ejercicio 1 con otro par de conjuntos que tengan el número cardinal 4.
3. Repetir el Ejercicio 1 con el número cardinal 10.
4. Repetir el Ejercicio 1 con el número cardinal 20.

1-2 LOS NUMEROS CARDINALES. Si para un conjunto dado S de elementos existe un número entero positivo N tal que los elementos de S puedan coordinarse en correspondencia biunívoca con el conjunto de los enteros positivos $1, 2, \ldots, N$, decimos que S es un *conjunto finito* con el número cardinal (finito) N. Si no existe un número entero positivo N que tenga esta propiedad, y si S tiene, por lo menos, un elemento, de-

cimos que S es un *conjunto infinito*. El número cardinal de cualquier conjunto finito puede obtenerse contando los elementos del conjunto, es decir, corresponde al mayor número ordinal que se necesita para contar los elementos del conjunto. El concepto de número cardinal considerado como un representante cualquiera de una clase de conjuntos permite asociar números cardinales transfinitos con conjuntos infinitos (Cap. 1-13).

Las comparaciones entre números cardinales deben concordar con las comparaciones correspondientes entre los conjuntos de elementos representados por los números cardinales. En efecto, los números cardinales a, b, que representan los conjuntos A, B, son iguales (se escribe $a = b$) y se dice que los conjuntos son *equivalentes* si existe una correspondencia biunívoca entre los elementos de los dos conjuntos. El número cardinal a es *menor que* el número cardinal b (se escribe $a < b$) y b es *mayor que* a (se escribe $b > a$), si después de asociar cada elemento de A con un elemento de B (uno a uno) queda, por lo menos, un elemento de B, al que no le corresponde ningún elemento de A, y no existe entonces una correspondencia biunívoca entre los elementos de B y los elementos de A. La segunda condición es superflua, en el caso de los conjuntos finitos, pero necesaria para los conjuntos infinitos. Por ejemplo, si ambos conjuntos A y B comprenden al conjunto de todos los números enteros positivos n, existe una correspondencia biunívoca (n a n) de cada entero consigo mismo y el conjunto A tiene el mismo número cardinal que el conjunto B. Sin embargo, se puede establecer, también, una correspondencia biunívoca (n a $2n$) entre todos los números enteros de A y los números enteros pares de B. En esta correspondencia entre dos conjuntos infinitos quedan elementos de B (los números enteros impares) que no corresponden a ningún elemento de A. Consideraremos este problema en forma más detallada en nuestro estudio sobre los números cardinales transfinitos (Cap. 1-13). Como ejemplo para el caso de conjuntos finitos, sean A el conjunto de alumnos de una clase, y B el conjunto de sillas de la sala de clases. Si cada alumno tiene una silla y cada silla está ocupada por un alumno, entonces $a = b$. Si cada alumno tiene una silla y, por lo menos, queda una silla sin ocupar, entonces $a < b$. Si todas las sillas están ocupadas y, por lo menos, un alumno no tiene silla, entonces $a > b$.

Un conjunto de elementos B se llama *subconjunto* de un con-

junto A, si cada elemento de B es un elemento de A; y se llama un *subconjunto propio* si es un subconjunto y hay, por lo menos, un elemento de A que no es un elemento de B. Un conjunto que no contiene ningún elemento es un *conjunto vacío o nulo* y se considera como un subconjunto de cualquier conjunto. Usando esta terminología, $a = b$ si A es equivalente a un subconjunto de B, y B es equivalente a un subconjunto de A; $a < b$ si A es equivalente a un subconjunto propio de B y B no es equivalente a ningún subconjunto de A. Dados dos conjuntos finitos A y B cualesquiera con números cardinales a, b, podemos comparar los números cardinales por medio de los subconjuntos 1, 2, ..., a y 1, 2, ..., b del conjunto de los números enteros positivos. Sea C el conjunto 1, 2, ..., c de números enteros positivos que se encuentran en ambos subconjuntos. Si $c = a$ y $c \neq b$, entonces $a < b$. Si $c = a$ y $c = b$, entonces $a = b$. Si $c = b$ y $c \neq a$, entonces $b < a$. De esta manera, hemos demostrado que para dos conjuntos finitos A y B cualesquiera con números cardinales a, b, debe ser válida exactamente una de las relaciones siguientes: $a < b$, $a = b$, o bien, $a > b$.

El ejemplo anterior de los alumnos, puede ampliarse para ilustrar la suma de los números cardinales. Sea G^* el conjunto de niñas de la clase, B^* el conjunto de niños, C^* el conjunto de sillas y g, b, c los números cardinales respectivos de estos conjuntos. Si cada estudiante tiene una silla y cada silla está ocupada por un estudiante, entonces, $c = g + b$. En general, dados los conjuntos A, B, C, en que A y B no tienen elementos en común (es decir, que los conjuntos A y B son *mutuamente exclusivos*), podemos escribir $a + b = c$, cuando existe una correspondencia biunívoca entre los elementos de C y la totalidad de los elementos de A y B; en otras palabras, C es equivalente a $A + B$ en que la suma de conjuntos ha de entenderse en el sentido de la teoría de conjuntos, como *totalidad de los elementos*. De esta manera, puede comprenderse fácilmente la adición de dos números cardinales cualesquiera por medio de correspondencias biunívocas. También se puede definir la multiplicación de los números cardinales. La sustracción y la división se pueden definir sólo en casos especiales. Por ejemplo, se puede escribir $c - b = a$, si y sólo si existe un número cardinal a tal que $c = a + b$.

*En inglés G de *girl*, niña; B de *boy*, niño; y C de *chair*, silla. (N. de la T.).

El producto de dos números cardinales, así como el producto de dos números enteros positivos, puede expresarse utilizando el concepto de adición sucesiva: $1 \cdot a = a$, $2 \cdot a = a + a$, $3 \cdot a = a + a + a$, ... Si el número de niños es igual al número de niñas en la clase a que nos referíamos anteriormente, entonces $g = b$ y $c = b + b = 2 \cdot b$. En este caso, el producto $ab = 2b$ es el número cardinal de un conjunto C equivalente a la suma de la totalidad de los elementos del conjunto C_1 de sillas ocupadas por las niñas y del conjunto C_2 de sillas ocupadas por los niños. En general, se escribe $c = ab$, siempre que C sea equivalente a la suma de la totalidad de los elementos de los conjuntos $C_1, C_2, \ldots, C_a$ mutuamente exclusivos; cada C_i es equivalente a B, y existe una correspondencia biunívoca (que se ha señalado con subíndices) entre los elementos de A y el conjunto de conjuntos C_i. En el ejemplo anterior, C es equivalente a $B + G$, B es equivalente a G, y existe una correspondencia biunívoca entre los elementos de A, por ejemplo, a_1, a_2, y el conjunto compuesto de los elementos B, G. Se puede escribir también $c/b = a$, siempre que $c = ab$.

Las *cuatro operaciones racionales* (adición, sustracción, multiplicación y división) se examinarán ampliamente en el presente texto. En el caso de los números cardinales, se ha visto que la suma de dos números cardinales cualesquiera es un número cardinal; la diferencia entre dos números cardinales es un número cardinal, para los casos en que esté definida; el producto de dos números cardinales cualesquiera es un número cardinal; y el cuociente de dos números cardinales es un número cardinal, siempre que esté definido previamente. Además, nuestras definiciones bastan para permitirnos probar que: a) los números cardinales satisfacen las relaciones corrientes de orden para los números enteros positivos (Ejercicios 7 y 8); y b) que la suma (Ejercicio 9) y la multiplicación (Ejercicio 10) de números cardinales tienen las mismas propiedades básicas que se atribuyen a la suma y multiplicación de los números enteros positivos (Cap. 1-5).

Antes de considerar las propiedades de los números enteros positivos convendría examinar, brevemente, los términos "operación" y "relación". Dado cualquier par de elementos a, b de un conjunto S, a menudo se asocia con ellos otros elementos, tales como $a + b$, $a - b$, $a \cdot b$, a/b de S. Tales operaciones se llaman *operaciones binarias* en S. En general, un conjunto S *es cerrado* bajo

una operación binaria $\oplus$, y la operación está *univocamente determinada* sobre el conjunto S, si para todos los elementos a, b de S, el elemento $a \oplus b$ es un elemento único de S. Las operaciones binarias de suma y multiplicación ya se han definido sobre el conjunto de números cardinales.

También se pueden comparar dos elementos a y b de un conjunto S. Por ejemplo, $a > b$ y $a = b$ indican comparaciones o *relaciones binarias* entre los elementos de S. Una relación binaria $\ominus$ está definida sobre un conjunto S, si para todo par ordenado (a, b) de elementos de S, puede determinarse si la relación es válida o no. Se dará por aceptado que cualquiera relación binaria debe ser válida o no serlo. Básicamente, supondremos que dados dos números cualesquiera a, b precisamente debe ser válida una de las relaciones $a = b$, o $a \neq b$. En este texto nos ocuparemos de las operaciones binarias y las relaciones binarias. En general, el conjunto S estará determinado: el conjunto S podría ser un conjunto particular de números o un conjunto de polinomios de ciertas variables definidas con coeficientes pertenecientes a un conjunto particular de números. Nos preocuparemos de definir o de indicar las características de todas las relaciones empleadas, teniendo en cuenta sus propiedades fundamentales, es decir, se establecerán propiedades de la relación tales, que todas las proposiciones en que aparezca la relación, serán válidas para todas las relaciones que tengan estas propiedades.

Las operaciones binarias de adición y multiplicación se tratarán de la manera ya descrita, es decir, se intentará caracterizar estas operaciones mediante sus propiedades básicas. En efecto, el desarrollo del sistema de números considerado en este capítulo, es esencialmente una consideración de las propiedades básicas de las relaciones de equivalencia, de los números enteros positivos, de la adición, de la multiplicación, de las relaciones de orden, de los números inversos, de las operaciones inversas, de los números racionales positivos, de los números negativos, de los números reales y de los números complejos. El orden de las materias en este estudio sigue fielmente aquél de la evolución histórica de nuestro sistema de números. La forma de postulados en que se presenta la materia obedece a una formalización matemática relativamente moderna que acentúa los conceptos fundamentales sobre los que se basa el álgebra (véase Bibliografía Nº 10, págs. 221-232). El

modo de abordar la teoría de los conjuntos es también comparativamente reciente (véase Bibliografía Nº 28). En el Nº 17 de la Bibliografía, se encontrará una relación no técnica del desarrollo del concepto de número con muchas anécdotas históricas.

EJERCICIOS

1. Dar un ejemplo de suma de números cardinales utilizando conjuntos de elementos.

2. Dar un ejemplo de sustracción de números cardinales, utilizando conjuntos de elementos.

3. ¿Está determinado $a - b$ para todos los números cardinales? Explicar.

4. Proponer un ejemplo de conjuntos A, B, que satisfagan las siguientes condiciones: (a) $a = b$; (b) $a = 2b$; (c) $a = 4b$; (d) $a < b$.

5. Citar un ejemplo de conjuntos A, B, que satisfagan las siguientes condiciones: (a) que $a - b$ esté definido; (b) que $a - b$ no esté definido; (c) que a/b esté definido; (d) que a/b no esté definido.

6. Valiéndose de sus conocimientos sobre números enteros, indique una correspondencia biunívoca entre los números enteros positivos y (a) los números enteros positivos pares; (b) los números enteros negativos; (c) los números enteros positivos múltiplos de diez; (d) las potencias enteras positivas de dos.

7. Demostrar que para números cardinales a, b, c, cualesquiera se verifica (a) si $a < b$ y $b < c$, entonces $a < c$; (b) si $a < b$, entonces $a + c < b + c$; (c) si $a < b$, entonces $ac < bc$.

8. Definir $a \overset{\cdot}{\geq} b$ para números cardinales a, b, cualesquiera y repetir el Ejercicio 7 para la relación $\overset{\cdot}{\geq}$

9. Demostrar que para números cardinales a, b, c, cualesquiera: (a) $a + b$ es un número cardinal único; (b) $a + b = b + a$; (c) $(a + b) + c = a + (b + c)$.

10. Demostrar que para números cardinales a, b, c cualesquiera: (a) ab es un número cardinal único: (b) $ab = ba$; (c) $(ab)c = a(bc)$; (d) $(a + b)\ c = ac + bc$.

1-3 RELACIONES DE EQUIVALENCIA.

Toda relación que tenga las tres propiedades siguientes, es decir, que sea:

reflexiva, $a = a$,
simétrica, $a = b$ implica $b = a$,
transitiva, $a = b$ y $b = c$ implican $a = c$,

se llama una *relación de equivalencia.* Puede demostrarse, como se indica a continuación, que la equivalencia de conjuntos es una relación de equivalencia y, por lo tanto, que la igualdad de números cardinales, tal como se define en el Cap. 1-2, también lo es: es reflexiva, puesto que los elementos de cualquier conjunto pueden ordenarse en correspondencia biunívoca con ellos mismos; es simétrica, dado que cualquiera correspondencia biunívoca entre los elementos de un conjunto A y los elementos de un conjunto B, puede también considerarse como una correspondencia biunívoca entre los elementos del conjunto B y los del conjunto A. Por último, es transitiva, ya que una correspondencia biunívoca entre los elementos de un conjunto A y aquellos de un conjunto B y

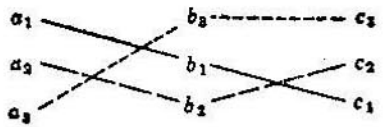


FIG. I–1

una segunda correspondencia biunívoca entre los elementos de B y aquellos de un conjunto C, dan origen a una correspondencia biunívoca entre los elementos de A y aquellos de C. Por ejemplo, en el caso de conjuntos finitos, si designamos los elementos correspondientes de A, B, C por a_1, b_1, c_1, respectivamente, obtenemos correspondencias similares a aquellas que se indican en la Fig. 1-1.

También se puede demostrar, empleando las definiciones acostumbradas, que la "identidad" ($\equiv$), la "congruencia" ($\cong$) de figura geométricas, y la "semejanza" ($\backsim$) de figuras geométricas son relaciones de equivalencia. De esta manera, cada uno de los símbolos $=$, $\equiv$, $\cong$, $\sim$ representa "igual a" en un sentido matemático bien definido. Ahora nos serviremos de la relación de equivalencia $=$ para describir las características de los números enteros positivos mediante los postulados de Peano. Como se señaló en el Cap. 1-2, se da por aceptado que dados dos números a y b, debe verificarse exactamente una de las dos relaciones $a = b$, $a \neq b$.

EJERCICIOS

1. ¿Expresa el signo $<$ una relación de equivalencia? Explicar

2. Demostrar que la semejanza de figuras en geometría plana es una relación de equivalencia.

3. ¿Representa el signo $\neq$ una relación de equivalencia? Explicar.

4. Determinar cuáles de las siguientes relaciones entre estudiantes son relaciones de equivalencia: (a) tener la misma edad, por ejemplo: Ruth tiene la misma edad que Juan; (b) ser mayor; (c) tener por lo menos la misma edad que...; (d) tener el mismo peso; (e) tener pesos diferentes; (f) tener mejores calificaciones; (g) tener en común una característica cualquiera dada; (h) no tener en común una característica dada.

5. La propiedad de las personas de ser diferentes, ¿es una relación de equivalencia? Explicar.

6. Dar un ejemplo de una relación que sea transitiva, pero que no sea reflexiva ni simétrica.

7. Dar un ejemplo de una relación que sea reflexiva y transitiva, pero no simétrica.

8. Dar un ejemplo de una relación que sea simétrica pero no sea reflexiva ni transitiva.

9. Demostrar que, considerado como conjunto de elementos, el conjunto de los números enteros positivos es equivalente al conjunto de las potencias enteras positivas de diez.

10. Ilustrar la equivalencia entre el conjunto de puntos de un segmento de recta de una unidad de longitud y el conjunto de puntos de un segmento de recta de diez unidades de longitud.

11. Ilustrar la equivalencia entre el conjunto de puntos de una recta y el conjunto de puntos de una circunferencia a la cual se le ha suprimido un punto.

12. Ilustrar la equivalencia entre el conjunto de puntos de un plano y el conjunto de puntos de una esfera a la cual se le ha suprimido un punto.

I-4 LOS POSTULADOS DE PEANO.

Ahora, vamos a iniciar el estudio de nuestro sistema de números siguiendo un orden lógico. En esta sección se formularán, primero, cinco propiedades que pueden usarse para distinguir a los números enteros positivos; en seguida, se dará por aceptado que los números enteros positivos tienen estas propiedades (es decir, estas propiedades se considerarán como postulados para el desarrollo de nuestro sistema de números) y finalmente se empleará uno de estos postulados para obtener un procedimiento formal para demostrar que una relación es válida para todos los números enteros positivos. Las cinco proposiciones siguientes se conocen con el nombre de *postulados de Peano:*

(i) 1 es un entero positivo.

(ii) A cada entero positivo a le corresponde como sucesor un entero positivo único a^+.

(iii) A ningún entero positivo le corresponde 1 como sucesor.

(iv) Si $a^+ = b^+$, entonces $a = b$.

(v) Todo conjunto de enteros positivos que contenga a 1 y al sucesor de todo entero positivo del conjunto, contiene a todos los enteros positivos.

El postulado (v) suele llamarse el *principio de inducción completa* y constituye la base del principio de inducción matemática. Ya que todo entero positivo a tiene un sucesor a^+, no existe un entero positivo mayor que todos los demás y no es posible verificar, por separado, ninguna relación para cada uno y para todos los enteros positivos. Por consiguiente, para demostrar que una relación o proposición es válida para todos los enteros positivos n necesitamos aplicar el principio de inducción completa. Más específicamente, consideramos el conjunto S de enteros positivos para el cual la proposición se verifica (es válida). Si 1 pertenece al conjunto S y, para cada entero positivo k de S, el entero $k^+ = k + 1$ pertenece también a S, entonces, según el principio de inducción completa, todos los números enteros positivos pertenecen al conjunto S, es decir, la proposición es válida para todos los números enteros positivos. He aquí el *principio de inducción matemática:*

Si una proposición $P(n)$ está definida para todos los valores enteros positivos de n de tal manera que $P(1)$ sea válido y que la validez de $P(k)$ implique la validez de $P(k + 1)$ para un valor entero positivo de k elegido arbitrariamente, entonces $P(n)$ es válida para todos los valores enteros positivos de n.

Aquí vamos a hacer una digresión y consideraremos un ejemplo de este principio, aun cuando técnicamente algunas de las operaciones y símbolos, tal como n^2, aún no han sido definidos. Supongamos que la proposición $P(n)$ sea

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

Para $n = 1$ se tiene $P(1): 1 = 1$, lo que es válido. En seguida, sea k cualquier número entero positivo tal que $P(k)$ sea válida, es decir,

$$1 + 3 + 5 + \ldots (2k - 1) = k^2;$$

sumando $2k + 1$ a ambos miembros de esta ecuación, queda demostrada la validez de $P(k + 1)$:

$$1 + 3 + \ldots + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2.$$

Luego, según el principio de inducción matemática, la proposición anterior $P(n)$ es válida para todos los valores enteros positivos de n. Otros ejemplos de la aplicación de este principio pueden encontrarse en el conjunto siguiente de ejercicios.

EJERCICIOS

Demostrar las proposiciones de los Ejercicios 1 a 3 aplicando los postulados de Peano. Demostrar las relaciones de los Ejercicios 4 a 9, aplicando el principio de inducción matemática.

1. Si $a \neq b$, entonces $a^+ \neq b^+$.
2. $a^+ \neq a$.
3. Todo entero positivo $a \neq 1$ es de la forma b^+, en que b es un entero positivo.

4. $2 + 4 + 6 + \cdots + 2n = n(n + 1)$.
5. $3 + 6 + 9 + \cdots + 3n = \dfrac{3n(n + 1)}{2}$.
6. $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n + 1)(2n + 1)}{6}$

7. $x - y$ es factor de $x^n - y^n$, siendo n un entero positivo cualquiera.
8. $x^{2n} - y^{2n}$ es divisible por $x + y$, siendo n un número entero positivo cualquiera.
9. $x^{mn} - y^{mn}$ es divisible por $x^m - y^m$ en que m y n son números enteros positivos cualesquiera.

I-5 LA ADICION Y LA MULTIPLICACION. Los postulados de Peano no bastan para definir la adición y la multiplicación explícitamente, pero pueden emplearse para demostrar que cada una de estas operaciones puede definirse exactamente de una manera única que satisfaga ciertas condiciones. Por ejemplo, puede demostrarse (Véase Bibliografía Nº 31; págs. 4-5) que dados dos números enteros positivos cualesquiera a, b, se

puede definir unívocamente un número entero positivo $a + b$, de modo que

$$a^+ = a + 1$$

para todo entero positivo a, y

$$a + b^+ = (a + b)^+$$

para todo par de enteros positivos a, b. Estas dos propiedades de la adición y los postulados de Peano pueden, por esta razón, aplicarse para demostrar que la adición de los números enteros positivos es única, asociativa y conmutativa, es decir,

(i) si a y b son números enteros positivos, existe un entero positivo único c tal que $a + b = c$;

(ii) $(a + b) + c = a + (b + c)$; y
(iii) $a + b = b + a$.

Se indicarán los procedimientos empleados para demostrar estas propiedades. Un examen acabado de esta materia puede encontrarse en el Nº 31 de la Bibliografía; págs. 3-8.

Se demostrará primero que $a + b$ es único para todos los enteros positivos a, b. Sea a un número entero positivo elegido arbitrariamente, pero fijo, y S el conjunto de enteros positivos b tales que $a + b$ sea un entero positivo determinado unívocamente. Por definición y de acuerdo con el segundo postulado de Peano, 1 pertenece a S, ya que $a^+ = a + 1$ es un número entero positivo unívocamente determinado. Si b pertenece a S, entonces $(a + b)^+$ se encuentra unívocamente determinado (segundo postulado de Peano), y b^+ pertenece a S dado que $a + b^+ = (a + b)^+$, de acuerdo con la segunda propiedad de la definición de adición. Por lo tanto, S contiene a todos los números enteros positivos, y $a + b$ es un entero positivo unívocamente determinado para todos los números enteros positivos a, b.

La demostración de que la adición es asociativa se obtiene de un modo similar (Ejercicio 1, más adelante) probando que el conjunto R de enteros positivos c tales que $(a + b) + c = a + (b + c)$ contiene a todos los enteros positivos.

Para demostrar que la adición es conmutativa se requiere dos veces el empleo del principio de inducción completa. Se demuestra primero que $a + 1 = 1 + a$ para todo entero positivo a y luego que $a + b = b + a$ para todos los números enteros positivos a, b. Sea T el conjunto de números enteros positivos a tales que $a + 1 = 1 + a$. El entero 1 pertenece a T dado que $1 + 1 = 1 + 1$. Si a pertenece a T, luego $a + 1 = 1 + a$ y dado que ya se ha demostrado la asociatividad de la adición, se puede aplicar la segunda propiedad de la definición de la adición dos veces y obtener $a^+ + 1 = (a + 1) + 1 = a + (1 + 1) = a + 1^+ = (a + 1)^+ = (1 + a)^+ = 1 + a^+$. Por lo tanto T contiene a^+ y de acuerdo con el principio de inducción completa, el conjunto T contiene a todos los números enteros positivos. Por último, sea a un número entero positivo constante elegido arbitrariamente y sea U el conjunto de los enteros positivos b tales que $a + b = b + a$. Acabamos de demostrar que 1 pertenece a U. Para cualquier número entero positivo b de U, tenemos que $a + b^+ = a + (b + 1) = (a + b) + 1 = 1 + (a + b) = 1 + (b + a) = (1 + b) + a = (b + 1) + a = b^+ + a$, de donde U contiene a todos los números enteros positivos (Ejercicio 2) y se ha demostrado que la adición es conmutativa.

Nos hemos servido de los postulados de Peano y de las dos propiedades de la adición que figuran en la definición de la adición para demostrar que la adición de dos enteros positivos es única, asociativa y conmutativa. Estas cinco propiedades de la adición se usarán extensamente en el desarrollo de nuestro sistema de números. Por ejemplo, se puede demostrar ahora la ley cancelativa de la adición, es decir, que $a + b = a + c$ implica $b = c$ (Ejercicio 3).

El tratamiento de la multiplicación que aquí se indica es muy similar al de la adición. Puede demostrarse (véase Bibliografía Nº 31; págs. 14-15) que, dados dos números enteros positivos a, b cualesquiera, se puede definir unívocamente un número entero positivo que se escribe $a \cdot b$ y también frecuentemente ab, de tal manera que

$$a \cdot 1 = a$$

para todo entero positivo a, y

$$a \cdot b^+ = ab + a$$

para todo par de enteros positivos a, b. Estas dos propiedades de la multiplicación y los postulados de Peano pueden emplearse ahora para demostrar que la multiplicación de los números enteros positivos es única (Ejercicio 6), distributiva con respecto a la adición (Ejercicios 8 y 11), asociativa (Ejercicio 9), y conmutativa (Ejercicios 7 y 10). También se puede demostrar la ley cancelativa de la multiplicación, es decir, que $ab = ac$ implica $b = c$ para números enteros positivos arbitrarios a, b, c (Ejercicio 12). Se dice que un entero d tiene un *factor o divisor* b si y sólo si existe un número entero a tal que $d = ab$. La ley cancelativa de la multiplicación establece por consiguiente que si $d = ab$ y $d = ac$, luego $b = c$.

La *notación exponencial* a^b en que a, b son números enteros positivos cualesquiera, se define como el producto $aaa \ldots a$ de b factores a. Según esta definición $a^b \cdot a^c = a^{b+c}$; si $a = d$, resulta $a^b = d^b$ (Ejercicio 16), y $a^b = d^b$ implica $a = d$ (Ejercicio 17), en que a, b, d son números enteros positivos elegidos arbitrariamente.

La definición $a \cdot 1 = a$ y la ley cancelativa de la multiplicación implican que si $ab = a$, entonces $b = 1$. La propiedad $a \cdot 1 = 1 \cdot a = a$ del número entero positivo 1 (Ejercicio 7) se indica estableciendo que 1 es la unidad, o sea, la *identidad con respecto a la multiplicación*. En general, la *identidad con respecto a una operación* es un elemento que, cuando se aplica a cualquier número de un conjunto dado mediante la operación dada, deja al número invariable. Nos referiremos en forma particular a los elementos de identidad de la adición y de la multiplicación.

Si existiera un número entero positivo b tal que $a + b = a$, entonces tendríamos que $(a + b)^+ = a^+$; $a + b^+ = a + 1$; y $b^+ = 1$, contrariamente al tercer postulado de Peano. Por lo tanto, no existe la identidad con respecto a la adición en el conjunto de los números enteros positivos. En consecuencia, ampliaremos ahora el concepto de "número" e incluiremos un símbolo que no es un entero positivo y definiremos este nuevo símbolo *0*, llamado cero, de tal manera que $a + 0 = a$ y $a \cdot 0 = 0$, donde a es cualquier número entero positivo o cero. Denominaremos a cero un número entero, pero teniendo presente que no es un entero positivo. En consecuencia (Ejercicio 18), con excepción de la ley cancelativa de la multiplicación, las propiedades básicas de la adición y de la multiplicación se verifican para el conjunto de números que comprende a los nú-

meros enteros positivos y cero, es decir, el conjunto de los *enteros no negativos.*

La propiedad $a \cdot 0 = 0$ para cualquier número entero no negativo a y el principio de inducción matemática pueden servir para demostrar que $0^b = 0$ para cualquier entero positivo b (Ejercicio 15). El símbolo 0^0 es *indefinido,* es decir, no tiene un significado específico en nuestro sistema de números. Para cualquier número entero positivo a, se define $a^0 = 1$, con el objeto de conservar la propiedad $a^b a^c = a^{b+c}$ para todos los enteros no negativos b, c. Hasta aquí se ha examinado la igualdad, la adición y la multiplicación de los números enteros positivos. Si a y b son números enteros positivos, resulta que $a = c$, $a + b = d$, y $a \cdot b = e$ son también números enteros positivos, es decir, el conjunto de números enteros positivos es cerrado (Cap. 1-2) con respecto a estas operaciones. En otras palabras, las ecuaciones $a = x$, $a + b = y$, y $a \cdot b = z$ tienen todas soluciones dentro del conjunto de los números enteros positivos. Ya se ha visto que la solución de $a + x = a$ no es un entero positivo. Antes de definir nuevos números con el objeto de encontrar las soluciones de $ax = b$, y $a + x = b$, se considerará un caso especial del segundo problema. En particular, se considerará una ordenación $a < b$ de los números enteros positivos tal que $a < b$ y $b > a$ todas las veces que $a + x = b$ tenga una solución dentro del conjunto de los números enteros positivos.

EJERCICIOS

1. Demostrar que la adición de los números enteros positivos es asociativa.

2. En el ejercicio anterior, al demostrar que la suma es conmutativa, explicar la razón, en cada paso de la demostración, por qué U contiene a todos los números enteros positivos.

3. Demostrar que $a + b = a + c$ implica $b = c$ para números enteros positivos cualesquiera a, b, c.

4. Demostrar que si $a = b$, entonces $a^+ = b^+$ y $a + c = b + c$, en donde c es cualquier número entero positivo.

5. Demostrar que $a = b$ y $c = d$ implican que $a + c = b + d$.

6. Demostrar que ab es un número entero positivo único para números enteros positivos a, b cualesquiera.

7. Demostrar que $a \cdot 1 = 1 \cdot a = a$ para todo número entero positivo a.

8. Demostrar que la multiplicación permanece distributiva con respecto a la adición, es decir, $a(b + c) = ab + ac$.

9. Demostrar que la multiplicación es asociativa, es decir, $(ab)c = a(bc)$.

10. Demostrar que la multiplicación es conmutativa, es decir, $ab = ba$.

11. Demostrar que la multiplicación es distributiva con respecto a la adición, es decir, $a(b + c) = ab + ac = (b + c)a$.

12. Demostrar que $ab = ac$ implica $b = c$ para números enteros positivos cualesquiera a, b, c.

13. Demostrar que $a = b$, implica $ac = bc$, donde c es un número entero positivo cualquiera.

14. Demostrar que $a = b$ y $c = d$ implica $ac = bd$.

15. Demostrar que $0^b = 0$ se verifica para cualquier número entero positivo b.

16. Demostrar que $a = d$ implica $a^b = d^b$, en donde a, d son números enteros no negativos arbitrarios y b es cualquier entero positivo.

17. Demostrar que $a^b = d^b$ implica $a = d$, en que a y d son números enteros no negativos cualesquiera, y b es cualquier número entero positivo.

18. Demostrar que en el conjunto de números enteros no negativos, la suma es única, asociativa y conmutativa, y que la multiplicación es única, asociativa, conmutativa y satisface la ley de distributividad.

I-6 RELACIONES DE ORDEN. Los números cardinales se han ordenado principalmente conforme a la definición siguiente: $a < b$ si y sólo si existe un número cardinal c tal que $a + c = b$ (Cap. 1 - 2). Definiremos ahora una ordenación similar para el conjunto de los números enteros positivos y cero, es decir, para el conjunto de los números enteros no negativos. Dados dos números enteros no negativos cualesquiera a, b se dice que *a es menor que b* $(a < b)$ y que *b es mayor que a* $(b > a)$ si y sólo si existe un entero positivo c tal que $a + c = b$. De manera que $0 < b$ para todo número entero positivo b (Ejercicio 1), y $1 < b$ para todo número entero positivo $b \neq 1$ (Ejercicio 2).

Dados dos números enteros no negativos cualesquiera a, b, podemos considerar ahora tres relaciones binarias $a < b, a = b, a > b$. Sea T el conjunto de números enteros no negativos a tales que se verifique exactamente una de las relaciones $a < b, a = b, a > b$, para todos los números enteros no negativos b. De acuerdo con lo señalado en el Cap. 1 - 3 se dará por sentado que dados dos enteros a, b, cualesquiera se verifica exactamente una de las relaciones $a = b, a \neq b$. Para $a = 0$, se obtiene $0 = b$ si $b = 0$ y $0 < b$ para $b \neq 0$. Para $a = 1$ se obtiene $b < 1$ si $b = 0$, $1 < b$ si $b \neq 0$ y $b \neq 1$. Para cualquier entero a de T se obtiene $b < a^+$ si $b < a$ o $b = a$; $b = a^+$ si $a < b$ y $a + 1 = b$; $a^+ < b$ si $a < b$ y $a^+ \neq b$.

Por consiguiente, de acuerdo con el principio de inducción matemática, todos los números enteros no negativos pertenecen al conjunto T. En otras palabras, dados dos números enteros no negativos cualesquiera a, b, es válida exactamente sólo una de las relaciones $a < b$, $a = b$, $a > b$.

La definición ya enunciada de $a < b$ para los números enteros no negativos se usará al definir $a < b$ para los números racionales positivos (Cap. 1-8), para los números negativos (Cap. 1-9) y para los números reales (Cap. 1-11). La ordenación de los números reales puede imaginarse fácilmente si se considera una correspondencia biunívoca entre el conjunto de los números reales y el conjunto de puntos de una recta según la geometría corriente de Euclides. El Axioma de Cantor-Dedekind (Cap. 1-12) establece esta correspondencia biunívoca. En este axioma se basa también el concepto de conjunto ordenado linealmente.

Un conjunto de elementos está *ordenado linealmente* si para elementos a, b del conjunto elegidos arbitrariamente

(i) $a \neq b$ implica $a < b$ o $b < a$;
(ii) $a < b$ implica $a \neq b$; y
(iii) $a < b$ y $b < c$ implican $a < c$.

Se ha dejado como un ejercicio para el lector el demostrar que el conjunto de números enteros no negativos está ordenado linealmente (Ejercicio 3). También puede demostrarse (Ejercicio 4) que exactamente una de las relaciones $a < b$, $a = b$, $a > b$ debe verificarse si a y b son elementos de cualquier conjunto ordenado linealmente.

La relación $<$ tiene varias propiedades más si a, b, c, d son números enteros no negativos cualesquiera. Por ejemplo,

(iv) $a < b$ implica $a + c < b + c$;
(v) $a < b$ y $c < d$ implican $a + c < b + d$;
(vi) $0 < c$ y $a < b$ implican $ac < bc$;
(vii) $a < b$ y $c < d$ implican $ac < bd$;
(viii) $1 < a$ y $b \neq 0$ implican $1 < a^b$;
(ix) $d \neq 0$ y $a < b$ implican $a^d < b^d$;
(x) $a <$ b y $1 < d$ implican $d^a < d^b$; y
(xi) $a < b$ y $1 < c < d$ implican $c^a < d^b$.

Las demostraciones de estas propiedades de los números enteros no negativos se dan como ejercicio (Ejercicio 5). Se considerará la validez y las modificaciones necesarias de estas propiedades a medida que nuestro concepto de número se amplíe y que las relaciones binarias $=$ y $<$ se definan para los números racionales positivos, para los números negativos y para los números reales.

EJERCICIOS

1. Demostrar que $0 < b$ para todo entero positivo b.
2. Demostrar que $1 < b$ para todo entero positivo $b \neq 1$.
3. Demostrar que el conjunto de números enteros no negativos está ordenado linealmente.
4. Demostrar que una de las relaciones $a < b$, $a = b$, $a > b$ debe ser válida exactamente si a, b son elementos de un conjunto ordenado linealmente.
5. Demostrar las propiedades (iv) a (xi) de la relación $<$ para los números enteros no negativos.
6. Se dice que un conjunto de elementos está *bien ordenado* si todo subconjunto *no vacío* (es decir, todo subconjunto que contiene por lo menos un elemento) tiene un primer elemento. Demostrar que el conjunto de números enteros no negativos es bien ordenado, es decir, demostrar que si un subconjunto de los números enteros no negativos contiene por lo menos un elemento, entonces contiene un elemento b tal que $b \leqq n$ para todo elemento n del subconjunto.

I-7 NUMEROS INVERSOS Y OPERACIONES INVERSAS. Usaremos las propiedades básicas de las relaciones y operaciones estudiadas anteriormente para ampliar nuestro conjunto de números y sus operaciones, introduciendo los conceptos de "números inversos" y "operaciones inversas". El inverso de un número n debe considerarse en relación con una operación binaria (Cap. 1-2) tal como la adición o la multiplicación. Se dice que los números 2 y $\frac{1}{2}$ son inversos entre sí con respecto a la multiplicación, ya que $2 \cdot \frac{1}{2} = 1$ y 1 es el elemento de identidad para la multiplicación (Cap. 1-5). También, dado que $2 + (-2) = 0$, se dice que 2 y -2 son inversos con respecto a la adición. En general, se dice que dos números a, a' son *elementos inversos* con respecto a una operación arbitraria $\oplus$ con un elemento de identidad p si y sólo si $a \oplus a' = p$. El adjetivo "inverso" puede también aplicarse a operaciones binarias. Dos operaciones pueden denominarse operaciones inversas si su efecto es

opuesto, esto es, si al aplicarse sucesivamente al mismo número, el número original permanece invariable. Por ejemplo $(5 + 2) - 2 = 5$ y también $(5 \cdot 2) : 2 = 5$. En conformidad con esta definición se dirá que la sustracción es la operación inversa de la adición y que la división es la inversa de la multiplicación. En general, se dice que dos operaciones binarias $\oplus$ y $\ominus$ *son operaciones inversas* si y sólo si $(a \oplus b) \ominus b = a$, donde a y b son elementos cualesquiera de algún conjunto de elementos para el cual las operaciones estén definidas. Para definir la división emplearemos esta relación y la propiedad por la cual para $b \neq 0$ se verifica $ab = cb$ si y sólo si $a = c$ (Ejercicios 12 y 13, Cap. 1 - 5). Se escribe $a : b = c$ si y sólo si $a = bc$. De la misma manera, para la *sustracción* se escribe $a - b = c$ si y sólo si $a = b + c$ (ver Ejercicios 3 y 4, Cap. 1 - 5).

Las relaciones entre los números inversos y las operaciones inversas también serán útiles en el estudio de nuestro sistema de números. Por ejemplo, $5 - 2 = 5 + (-2)$ y $5 \div 2 = 5 \cdot (1/2)$. En general, tenemos la relación $b \oplus a = b \ominus a'$ si dado cualquier elemento b y elementos inversos a y a' con respecto a una operación arbitraria $\oplus$ con inversa $\ominus$ siempre que ambas operaciones estén definidas para los elementos dados.

Ya hemos introducido las cuatro operaciones racionales, adición, sustracción, multiplicación y división. La adición y la multiplicación se rigen por las propiedades que se han determinado en el Cap. 1 - 5; la sustracción y la división (excluyendo la división por cero) se han definido como las inversas de la adición y la multiplicación, respectivamente. Podemos también considerar una forma abreviada de la multiplicación repetida, a saber, la *potenciación* (la elevación de una cantidad a una potencia dada), junto con su operación inversa, la *radicación* (extracción de raíz). De estas operaciones surge la necesidad de definir nuevos símbolos como números, es decir, de ampliar gradualmente el conjunto de los elementos en estudio. El conjunto de los enteros positivos es cerrado para la adición, para la multiplicación y con respecto a la potenciación. Al considerar la división se necesitan los números racionales positivos; los números racionales positivos y negativos y cero, al considerar la división y la sustracción. Para tratar la radicación se necesita un conjunto aún más amplio de números. La adición, la sustracción, la multiplicación, la división, la potenciación y la radi-

cación pueden definirse para los números enteros positivos en el conjunto de los números reales. Estudiaremos el conjunto de números complejos con el objeto de obtener un conjunto de números tales que estas seis operaciones puedan ser definidas para todos los elementos diferentes de cero del conjunto (en lugar de serlo solamente para los números enteros positivos).

Después de haber alcanzado esta visión panorámica de nuestro sistema de números, consideraremos nuevamente el conjunto de los números enteros positivos. El conjunto de los números enteros positivos es cerrado para la suma y para la multiplicación. No es cerrado para la sustracción ni para la división. Desde el punto de vista práctico los enteros positivos sirven para contar objetos o para comparar conjuntos finitos de objetos. Aún no hemos mencionado números que sirvan para representar cosas tales como, por ejemplo, la porción que una persona recibe cuando se dividen tres manzanas en partes iguales entre seis personas, o la temperatura relativa a la cual se congela el agua. Por lo tanto hay que ampliar el conjunto de los números incluyendo en él a las fracciones (Cap. 1 - 8) y a los números orientados, es decir, precedidos de los signos +, — (Cap. 1 - 9). En otras palabras, se necesitan números inversos para los números enteros positivos con respecto a la multiplicación y a la adición, junto con números que representen sumas de estos nuevos números.

EJERCICIOS

Demostrar cada uno de los siguientes ejercicios con respecto a los números enteros no negativos q, r, s, t elegidos arbitrariamente:

1. $r < s < t$ implica $t - s < t - r$.
2. $r < s < t$ implica $s - r < t - r$.
3. $q < r < s < t$ implica $s - r < t - q$.

1-8 LOS NUMEROS RACIONALES POSITIVOS. El número inverso del número entero positivo b con respecto a la multiplicación se define como un número b' tal que satisfaga la relación $bb' = 1$. Se dice que $b' = 1/b$ es la *solución o raíz* de la ecuación $bx = 1$. También se llama *el cero* del polinomio $bx - 1$. Definiremos, ahora, un conjunto nuevo de números, los *números racionales positivos,* a fin de que podamos

resolver ecuaciones de la forma $bx = a$ para cualquier entero positivo a y b. Estos números pueden representarse por pares a/b de enteros positivos y tienen las siguientes propiedades:

(i) $\dfrac{a}{b} = \dfrac{c}{d}$ si y sólo si $ad = bc$;

(ii) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$;

(iii) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$; y

(iv) $\dfrac{a}{b} < \dfrac{c}{d}$ si y sólo si $abd^2 < b^2cd$.

La condición $abd^2 < b^2cd$ en (iv) se puede enunciar en la forma $ad < bc$ todas las veces que bd sea positivo. La forma $abd^2 < b^2cd$ se usa aquí dado que permanecerá válida cuando ampliemos el conjunto de números (Cap. 1-3) incluyendo en él a los números negativos.

Los números racionales positivos de la forma $a/1$ se identifican con los números enteros a. Técnicamente, el conjunto de enteros positivos es *isomorfo* con respecto al conjunto de los números racionales positivos de la forma $a/1$, es decir, existe una correspondencia biunívoca entre $a/1$ y a que se conserva en la adición y en la multiplicación. [$a/1 + b/1$ corresponde a $a + b$ y $(a/1)(b/1)$ corresponde a ab]. Este isomorfismo particular se mantiene también con respecto a las relaciones de orden (dado que $a/1 < b/1$ si y sólo si $a < b$) y se llama *isomorfismo de orden*.

Se dice que los pares iguales de enteros tales como los que se especifican en (i) anteriormente, representan el mismo número racional. En el conjunto de todos los pares de enteros que son iguales a un par dado, existe un par, digamos a/b tal que si r/s es cualquier otro par del conjunto, resulta $r = ta$ y $s = tb$ para algún

entero positivo t. Puede hacerse una demostración rigurosa de la existencia del par a/b (Ejercicio 16), valiéndose del hecho de que el conjunto de enteros positivos es bien ordenado (Ejercicio 6, Cap. 1 - 6). Se dice que el par a/b es la *forma reducida* del número racional dado.

Las definiciones anteriores permiten demostrar que para los números racionales positivos, la adición es única, asociativa, y conmutativa y que la multiplicación es única, asociativa, conmutativa, y satisface la ley de distributividad, es decir, la adición y la multiplicación tienen las mismas propiedades básicas (Cap. 1 - 5) en el conjunto de los números racionales positivos que en el conjunto de los enteros positivos. Por ejemplo, la suma anterior de (ii) es única, dado que $ad + bc$ y bd son únicos para enteros positivos cualesquiera a, b, c, d. De la misma manera, de

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b},$$

resulta que la adición es conmutativa. Las demostraciones restantes se dan como ejercicios al final de esta sección.

Si e y f son números racionales positivos, entonces tal como en el caso de los enteros positivos, $e - f = g$ se define como un número racional positivo si y sólo si existe un número racional positivo g tal que $e = f + g$. Análogamente, $e/f = h$, se define como un número racional positivo si y sólo si existe un número racional positivo h tal que $e = fh$. El número g existe si y sólo si $f < e$ [ver Ejercicio 5 (a)]; el número h existe siempre (Ejercicio 6). Por consiguiente, los pares e/f de números racionales positivos son a su vez ellos mismos números racionales y nada nuevo puede obtenerse al considerar estos pares de números racionales en vez de pares de números enteros. La propiedad [Ejercicio 5 (b)] de que para dos números racionales cualesquiera e, f, que satisfagan la relación $e < f$, existe un número racional positivo r que cumple con la relación $e < r < f$, se indica diciendo que los números racionales positivos son *densos*, es decir, que entre dos números racionales positivos distintos cualesquiera existe un tercer número racional positivo. Los enteros positivos no son densos.

Ya se ha definido el símbolo a^b (Cap. 1 - 5) para el caso de que a y b sean números enteros no negativos y por lo menos uno de

ellos sea diferente de cero. El símbolo r^b donde r es cualquier número racional positivo y b es cualquier número entero no negativo puede definirse exactamente como en el caso de los enteros, es decir, $r^0 = 1$ y r^b para cualquier entero positivo b indica el producto de b factores r. Ahora especificaremos que el símbolo $r^{1/b}$ en donde r es cualquier número racional positivo y b es cualquier entero positivo, debe satisfacer la relación $(r^{1/b})^b = r$, es decir, el producto de b factores $r^{1/b}$ debe ser igual a r. De este modo se conservará la propiedad $a^b a^c = a^{b+c}$ para los nuevos símbolos. El símbolo $r^{d/b}$ donde $r > 0$, indica el producto de d factores $r^{1/b}$, y el producto $r^s r^t$ se expresa por el símbolo r^{s+t} para números racionales positivos cualesquiera. Si s no es un entero, los nuevos símbolos r^s pueden no ser números racionales y las relaciones entre ellos aún no se han definido formalmente.

Las soluciones de las ecuaciones $x = a + b$, $x = ab$, y $ax = b$ son números racionales positivos para números racionales positivos a, b, cualesquiera, es decir, el conjunto de números racionales positivos es cerrado con respecto a la adición, a la multiplicación y a la división. Hemos ampliado nuestro concepto de número para incluir $a + b$, ab, y a/b en donde a, b son enteros positivos cualesquiera o números racionales positivos arbitrarios. Ampliaremos en seguida nuestro concepto de número y definiremos nuevos símbolos como números considerando la expresión $a - b$ para los casos en que a, b sean números racionales positivos arbitrarios o cero, es decir, sean *números racionales no negativos.*

EJERCICIOS

1. Demostrar que la adición de números racionales positivos es asociativa.
2. Demostrar que la multiplicación de números racionales positivos es (a) única, (b) asociativa, (c) conmutativa, y (d) distributiva con respecto a la adición.
3. Demostrar que $ac/bc = a/b$, siendo a, b, c enteros positivos elegidos arbitrariamente.
4. Demostrar que $(a + c)/b = a/b + c/b$, en donde a, b, c son enteros positivos arbitrarios.
5. Demostrar que si $a/b < c/d$ en donde a, b, c, d son enteros positivos arbitrarios, entonces existe (a) un número positivo racional g tal que $a/b + g = c/d$; y (b) un número positivo racional r tal que $a/b < r < c/d$.
6. Dados números enteros positivos cualesquiera a, b, c, d, demostrar que existe un número racional positivo h tal que $a/b = (c/d) \cdot h$.

7. Determinar que la *media aritmética o promedio* de dos números racionales positivos cualesquiera a, b es $m = (a + b)/2$, y en el caso en que $a < b$, demostrar que $a < m < b$.

8. Definir la expresión $0/1 = 0$ basándose en la suposición de que las propiedades (i) a (iv) enunciadas anteriormente son válidas para pares de números enteros no negativos a/b, $b \neq 0$, y demostrar que $0 < r$ siendo r cualquier número racional positivo.

9. Demostrar que $a < b$ implica $1/b < 1/a$, en donde a, b son (a) cualquier entero positivo; (b) cualquier número racional positivo.

10. Demostrar que $a < b$ y $c < d$ implica $a/d < b/c$ en donde a, b, c, d son (a) enteros positivos cualesquiera, (b) números racionales positivos cualesquiera.

11. Demostrar que a/b y b/a son números inversos con respecto a la multiplicación para números enteros positivos a, b arbitrarios.

12. Encontrar los números inversos con respecto a la multiplicación, siempre que tales números existan para cada uno de los números siguientes: 3, 5, 1/10, 1, 0, 10, 200.

13. Discutir, empleando ejemplos, qué conjuntos de números se necesitan para (a) resolver ecuaciones lineales y cuadráticas; (b) para efectuar las seis operaciones descritas en el Cap. I — 7.

14. Demostrar que los números racionales positivos están ordenados linealmente (Cap. I — 6).

15. Volver a formular las once propiedades de la relación $<$ que aparecen en el Cap. I — 6 de modo de obtener las once propiedades de esta misma relación $<$ para el caso en que a, b, c, d sean números racionales no negativos.

16. Demostrar que todo número racional positivo puede expresarse en forma reducida*.

I - 9 LOS NUMEROS NEGATIVOS.

Acabamos de considerar como símbolos pares a/b de números enteros positivos: hemos definido la igualdad, la adición, y la multiplicación de estos símbolos; hemos demostrado que estas definiciones son consistentes con las definiciones anteriores aplicadas a un subconjunto de elementos $a/1$ isomorfo con el conjunto original de elementos a, y hemos obtenido nuevos números (los números racionales positivos) al aceptar todos los símbolos a/b como números en que a y b son enteros positivos. Repetiremos ahora este proceso considerando como símbolos pares $[a — b]$ de números racionales no negativos, definiendo la igualdad, la suma y la multiplica-

*Ver definición en páginas anteriores. (N. de la T.).

ción de estos nuevos símbolos, demostrando que el conjunto de símbolos $[a - 0]$ es isomorfo con el conjunto de números no negativos a de acuerdo con estas nuevas definiciones y aceptando luego, todos los pares de números racionales no negativos $[a - b]$ como números racionales: positivos, negativos y cero.

Se definirá primero las relaciones y operaciones siguientes respecto a estos nuevos símbolos donde a, b, c, d son números racionales no negativos arbitrarios:

$$\begin{aligned}
&\text{(i)} \quad [a - b] = [c - d] \text{ si y sólo si } a + d = b + c;\\
&\text{(ii)} \quad [a - b] + [c - d] = [(a + c) - (b + d)];\\
&\text{(iii)} \quad [a - b] \cdot [c - d] = [(ac + bd) - (bc + ad)];\\
&\text{(iv)} \quad [a - b] < [c - d] \text{ si y sólo si } a + d < b + c.
\end{aligned}$$

Tal como se ha hecho anteriormente, hemos definido el significado de las relaciones básicas $=$, $<$, y de las operaciones básicas $+$, $\cdot$ con respecto a los nuevos símbolos $[a - b]$. Demostraremos, ahora que la correspondencia entre $[a - 0]$ y a es un isomorfismo de orden (Cap. 1-8) y que las operaciones básicas tienen sus propiedades usuales en el conjunto completo de los pares de números $[a - b]$.

La correspondencia entre $[a - 0]$ y a es claramente biunívoca. Queda por demostrar que esta correspondencia subsiste respecto de la adición, de la multiplicación y en las relaciones de orden. Estas correspondencias pueden verificarse fácilmente dado que, por definición.

$$\begin{aligned}
&[a - 0] + [b - 0] = [(a + b) - (0 + 0)];\\
&[a - 0] \cdot [b - 0] = [(ab + 0) - (0 + 0)];\\
&[a - 0] < [b - 0] \text{ si y sólo si } a + 0 < b + 0.
\end{aligned}$$

Por consiguiente, el conjunto de las expresiones $[a - 0]$ donde a es un número racional no negativo es equivalente en el sentido de que es isomorfo con el conjunto de los números racionales no negativos.

Sean a, b en la expresión $[a - b]$ números racionales no negativos cualesquiera. Como en el caso de los números racionales positivos a/b, podemos probar que la suma de las expresiones $[a - b]$ es única, asociativa y conmutativa (Ejercicio 1), y que la multi-

plicación es única, asociativa, conmutativa y satisface la ley de distributividad (Ejercicio 2). En efecto, consideraremos todas las expresiones de la forma $[a - b]$ como números, *números racionales precedidos de signo,* en que a, b son números racionales no negativos arbitrarios. De acuerdo con el isomorfismo ya mencionado el número racional precedido de signo $[a - b]$ corresponde a 0 cuando $a = b$ y corresponde a d, cuando $a > b$ y $a = b + d$. Dado que una de las relaciones $a < b$, $a = b$, $a > b$, debe ser válida exactamente (Ejercicio, 4, Cap. 1-6 y Ejercicio 14, Cap. 1-8), necesitamos una expresión correspondiente análoga para $[a - b] = [0 - c]$ en donde $a < b$ y $a + c = b$. De consiguiente, definiremos ahora la expresión $[0 - c]$ como un *número racional negativo* y la expresión $[0 - c]$ la escribiremos $-c$. El número racional positivo c se denomina *valor numérico o valor absoluto* de $-c$ y de c, $c = |-c| = |c|$. Los números racionales positivos y negativos y el cero constituyen los números racionales precedidos de signo o simplemente los *números racionales.* Cuando a, b, son enteros positivos o cero, los pares $[a - b]$ pueden usarse de la misma manera que se hizo anteriormente para definir a los *enteros negativos.* Los números enteros positivos y negativos y el cero constituyen los *números enteros.*

Ya se ha definido la suma y la multiplicación para todos los números racionales. Se definirá ahora la sustracción y la división. La sustracción puede ser definida para números racionales arbitrarios por medio de la relación

$$[a - b] - [c - d] = [(a + d) - (b + c)]$$

(Ejercicio 3). La división de los números racionales puede definirse por

$$\frac{[a - b]}{[c - d]} = \left[\frac{ac + ad}{c^2 - d^2} - \frac{bc + bd}{c^2 - d^2}\right]$$

donde $c \neq d$. La división es indefinida cuando $c = d$. (Ejercicios 4 y 5). Estas definiciones nos permiten demostrar que

(i) $-a < -b$ si y sólo si $b < a$;
(ii) $a + (-b) = a - b$;
(iii) $(-a)b = a(-b) = -ab$; y
(iv) $(-a)(-b) = ab$,

para todos los números racionales a, b, no negativos. Por ejemplo, $-a < -b$ es por definición lo mismo que $[0 - a] < [0 - b]$ y nuevamente por definición esto es válido si y sólo si $0 + b < 0 + a$, esto es, si $b < a$. En forma análoga $a + (-b) = [a - 0] + [0 - b] = [(a + 0) - (0 + b)] = [(a - 0) - (b - 0)] = [(a - b) + (0 - 0)] = a - b$. Las dos demostraciones restantes constituyen el Ejercicio 6. Las demostraciones ponen en evidencia que las propiedades anteriores de los números precedidos de signo son una consecuencia de las definiciones enunciadas hasta ahora.

Podremos ahora ampliar la notación exponencial incluyendo exponentes negativos. Se define a^b como en el Cap. 1-8 para cualquier entero positivo b y para cualquier número racional a. También como anteriormente, $a^0 = 1$ para cualquier valor de $a \neq 0$. Para obtener una definición con respecto a los exponentes negativos es necesario que a^{-b} satisfaga la expresión $a^{-b}a^b = 1$ para cualquier entero b y para cualquier número racional a, excepto 0. De esta manera se conserva la propiedad $a^b a^c = a^{b+c}$ para todos los números racionales $a \neq 0$ y para todos los números enteros b, c. Aún no se ha definido explícitamente el símbolo a^b para valores no enteros de b. Se considerará este asunto en el Cap. 1-12. El símbolo 0^b es indefinido cuando b es negativo o cero.

El conjunto de todos los números racionales es cerrado con respecto a la adición, a la sustracción, a la multiplicación y a la división (excluyendo la división por cero), es decir, la suma, la diferencia, el producto y el cuociente (divisor diferente de cero) de dos números racionales arbitrarios son números racionales. A mucha gente le interesan principalmente los números racionales. Probablemente ellos bastan para la mayoría de los proveedores, oficinistas y aún banqueros. No obstante, los números racionales tienen también limitaciones bien determinadas. Por ejemplo, la distancia expresada en pies desde el "home plate" hasta la segunda base en baseball, y el diámetro en pulgadas de una pelota de baseball de nueve pulgadas de circunferencia, no pueden formularse con exactitud en números racionales. Pueden expresarse aproximadamente en números racionales, y el error en la aproximación puede hacerse menor que el producido por cualquier número racional positivo dado (de antemano).

La necesidad de ampliar el conjunto de los números racionales puede expresarse también en magnitudes. Hemos definido conjun-

tos finitos y números cardinales finitos (Cap. 1-2). Definiremos, ahora, un número d como un *número finito* si y sólo si existe un entero positivo N tal que $-N < d < N$. Se dice que cualquiera magnitud, cualquiera cantidad, cualquier objeto, cualquiera expresión algebraica, etc., es finita si se puede representar por o representa a un número finito. Necesitamos y por eso estudiaremos un conjunto de números, el conjunto de los números reales, que sirve para comparar magnitudes de dos objetos finitos similares cualesquiera. Toda magnitud finita puede representarse mediante un número real.

EJERCICIOS

1. Demostrar que la adición de los números racionales precedidos de signo es única, asociativa y conmutativa.

2. Demostrar que la multiplicación de los números racionales precedidos de signo es única, asociativa, conmutativa, y satisface la ley de distributividad.

3. Demostrar que la sustracción de los números racionales puede definirse mediante $[a - b] - [c - d] = [(a + d) - (b + c)]$ haciendo ver que según esta definición la sustracción es la operación inversa de la adición.

4. Demostrar que en el conjunto de los números racionales positivos y negativos (con exclusión del cero) la división tal como se definió anteriormente es la operación inversa de la multiplicación.

5. Demostrar que la división por cero no puede definirse en el conjunto de los números racionales.

6. Demostrar las propiedades indicadas en los números (ui) y (iv) para los números racionales.

7. Demostrar que $-c < 0$ para cualquier número racional positivo c.

8. Demostrar que $a < b$ y $c < 0$ implican $bc < ac$.

9. Indicar cuales de los ejercicios del Cap. 1 — 7 pueden demostrarse cuando q, r, s, t son números racionales arbitrarios (positivos, negativos o cero).

10. Demostrar, por medio de la expresión $a^{-n} = 1/a^n$ que para enteros q, r, y para números racionales s, t las relaciones $q < r < 0$ y $0 < s < t < 1$ implican $1 < t^r$, $t^r < t^q$, y $t^r < s^r$.

11. Obtener el número inverso con respecto a la adición para cada uno de los siguientes números: 3, −5, 1/10, 1, 0, 10, −200.

12. Hacer una lista de los números racionales que son sus propios inversos con respecto a la suma y a la multiplicación.

13. Demostrar que $[a - b]$ y $[b - a]$ son inversos con respecto a la adición para numeros racionales positivos a, b arbitrarios.

14. Demostrar que los números racionales están ordenados linealmente.

15. Formular de nuevo las once propiedades de la relación $<$ del Cap. I — 6 con el objeto de obtener las onces propiedades para $<$ cuando a, b, c, d son números racionales.

I-10 LOS NUMEROS REALES. El número asociado con un objeto o conjuntos de objetos representa comúnmente una medida o magnitud relativa a alguna unidad conocida, por ejemplo, la altura de un árbol en pies, la extensión de una hacienda en acres, o el número de manzanas de una caja (comparado con una manzana). Cuando la medida de un objeto en relación a otro no se puede expresar como un cuociente entre enteros, los dos objetos se llaman *inconmensurables*. Los griegos de la antigüedad observaron que la diagonal y el lado de un cuadrado son inconmensurables. La circunferencia y el diámetro de un círculo son también inconmensurables. Todo número que no pueda expresarse como cuociente entre dos enteros se llama *irracional*.

Probaremos ahora que $\sqrt{2}$ es irracional. Supongamos que $\sqrt{2} = a/b$, donde a y b son enteros que no tienen un factor común entero. Entonces $a^2 = 2b^2$, de aquí que resulte que a^2 es un entero par. Por lo tanto, dado que sólo un entero par puede tener un entero par como su cuadrado, a es divisible por 2. Sea $a = 2c$. Entonces resulta $4c^2 = 2b^2$, $2c^2 = b^2$, y b es divisible por 2, contrariamente a nuestra suposición de que a y b no tienen factores comunes enteros. Por lo tanto la primera suposición de que $\sqrt{2} = a/b$ es imposible, y $\sqrt{2}$ es un número irracional.

El método de demostración anterior suele denominarse método de *demostración directa* o *reductio ad absurdum*. Consiste en suponer que la conclusión deseada es falsa y en valerse de esta suposición y de la hipótesis dada para efectuar una demostración lógica de alguna aserción que sea contraria a la suposición o la hipótesis. (Ejercicio 1). En seguida se dice que puesto que la suposición conduce a una contradicción, la suposición debe ser falsa, es decir la conclusión deseada debe ser verdadera. Una forma de demostración indirecta de un teorema, por ejemplo, *(A* implica *B)* es la demostración directa del teorema *contrarrecíproco* ("no *B*" implica "no *A*"). El método de demostración indirecta puede considerarse también como un caso especial de demostración por eliminación (Ejercicio 4).

Los números irracionales tales como $\sqrt{2}$ pueden definirse de varias maneras. Nos alejaremos momentáneamente de nuestro tratamiento sistemático del sistema de números con el objeto de examinar brevemente la notación decimal para representar a todos los números reales (racionales e irracionales). En realidad, las definiciones de y las operaciones con decimales infinitos se basan sobre los mismos conceptos fundamentales de sucesiones infinitas y límites (Cap. III-11). Por el momento nuestras consideraciones serán algo intuitivas. Las definiciones rigurosas se harán en la sección siguiente en función de las cortaduras de Dedekind. Todos los conceptos intuitivos que se usan en esta sección pueden probarse rigurosamente basándose en las definiciones sistemáticas.

En el Cap. II-6 demostraremos que cualquier entero positivo N puede expresarse en la "base" 10 en la forma

$$N = d_k\, 10^k + d_{k-1}\, 10^{k-1} + \ldots + d_2\, 10^2 + d_1\, 10 + d_0,$$

donde los d_j son elementos del conjunto 0, 1, 2, ..., 9 de *dígitos* de la base diez. Por ejemplo, 1953 significa $1 \cdot 10^3 + 9 \cdot 10^2 + 5 \cdot 10 + 3$. Ciertas fracciones pueden expresarse en la forma:

$$N + a_1/10 + a_2/10^2 + \ldots + a_m/10^m,$$

donde N y m son enteros positivos y los a_j son dígitos. Por ejemplo, $123/4 = 30 + 7/10 + 5/10^2 = 30.75$. Concretamente, un número racional $r = a/b$ puede representarse por medio de un número finito de términos como en la notación decimal precedente (es decir, por medio de *un decimal exacto*) si y sólo si r es un entero o bien si $10^m r$ puede expresarse como número entero para algún número entero positivo m. Dado que $2^0 = 5^0 = 1$, esta condición puede formularse como sigue: un número racional r puede expresarse como un decimal exacto si y sólo si existen enteros a, p, q tales que $r = a/(2^p 5^q)$.

Se debe aceptar que el símbolo 1.333 ... es un número con el objeto de poder expresar el número racional 4/3 en notación decimal. En rigor, esto envuelve los conceptos de sucesiones infinitas y de límites. Decimales como el anterior o como $\frac{15}{7} = 2.142857142857$ ..., que consisten en conjuntos de dígitos, tal como el 3 en el caso

de $\frac{4}{3}$ y 142857 en el caso de $\frac{15}{7}$, repetidos indefinidamente se llaman *decimales periódicos infinitos.* También se puede considerar a los decimales exactos como decimales periódicos infinitos haciendo $a_j = 0$ para el valor j suficientemente grande. Por ejemplo, $0.25 = 0.2500000$ .... Demostraremos en el Cap. II-7 que todo número racional puede representarse como un decimal periódico infinito y, a la inversa, todo decimal periódico infinito, representa un número racional. Es fácil imaginarse la proposición conversa mediante el procedimiento siguiente: dado cualquier decimal periódico d en el que se repite indefinidamente un conjunto de k dígitos, calcular $10^k \cdot d - d$ y dividir por $10^k - 1$. Por ejemplo, si $d = 1.333...$, se calcula $10d - d = 13.333... - 1.333... = 12$, de donde $d = \frac{4}{3}$. Si $d = 0.164545...$, entonces $100d - d = 16.29$, de donde $d = 16.29/99 = 1629/9900$. Como se señaló anteriormente, una definición precisa de la sustracción de decimales infinitos requiere el concepto de límite.

Definiremos, ahora, un *decimal infinito* como la expresión:

$$N + a_1/10 + a_2/10^2 + \ldots + a_n/10^n + \ldots,$$

donde N es un entero y los a_j son dígitos. De las consideraciones anteriores se desprende que, una vez hechas las definiciones adecuadas, es posible demostrar que un subconjunto (los decimales periódicos infinitos) del conjunto de los decimales infinitos es isomorfo con el conjunto de los números racionales. En general, se puede definir la igualdad, la suma y el producto de decimales infinitos, de modo que todos los decimales infinitos se comportan como números. De esta manera, se puede representar números nuevos, *números irracionales,* tales como $\pi = 3.1415926536...$ (ver Bibliografía Nº 40, págs. 39-40), como *decimales infinitos no periódicos.* El conjunto de todos los decimales infinitos, es decir, el conjunto total de números racionales e irracionales, se llama el conjunto de los *números reales.* En consecuencia, si convenimos en que *todos los decimales infinitos representan números,* obtenemos el conjunto de los números reales. Dado que esta suposición, en último término, envuelve el concepto de límites de sucesiones infinitas, basaremos nuestro estudio sistemático del sistema de números reales sobre las cortaduras de Dedekind (Cap. I-11). Se ha se-

ñalado la Sección 11 del Cap. 1 como optativa para indicar que cualquier lector que desee aceptar las propiedades corrientes de los decimales infinitos sin una demostración rigurosa pueda prescindir de esa sección.

Los números reales pueden clasificarse de diversas maneras. Son positivos, negativos o cero. Son racionales o irracionales. Son algebraicos o trascendentes. Se dice que un número es *algebraico* si satisface alguna ecuación de la forma.

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0, \; a_0 \neq 0$$

donde los a son enteros y n es un entero positivo. De todos los demás números reales se dice que son *trascendentes*. Cualquier número racional a/b satisface la ecuación $bx - a = 0$, y, por lo tanto, es algebraico. Algunos números irracionales, como $\sqrt{2}$ que satisface la condición $x^2 - 2 = 0$, son algebraicos. También existen números algebraicos, tales como i y $-i$ que satisfacen la ecuación $x^2 + 1 = 0$, y que no son números reales. Un número algebraico real puede ser racional o irracional; todos los números reales trascendentes son irracionales. La base de los logaritmos naturales

$$e = \lim_{x \to 0} (1 + x)^{1/x}$$

es un número trascendente real; también lo es π, la razón entre la circunferencia y el diámetro de un círculo (ver Bibliografía Nº 29, págs. 71-89, 111). El símbolo πi, donde i satisface la ecuación $x^2 + 1 = 0$, representa un número trascendente que no es un número real.

EJERCICIOS

1. Dos proposiciones son *contrarias* si ambas no pueden ser verdaderas simultáneamente. Por ejemplo, las proposiciones "El automóvil es un Ford" y "El automóvil es un Dodge" son contrarias. Enunciar cinco pares de proposiciones contrarias.

2. Dos proposiciones son *contradictorias* si ambas no pueden ser verdaderas ni tampoco pueden ser ambas falsas. Las proporciones dadas en el ejemplo ilustrativo del Ejercicio 1, no son contradictorias, dado que ambas podrían ser falsas. Las proposiciones contradictorias son importantes, ya que si una es verdadera, la otra es falsa; y si una es falsa, la otra es verdadera. Formular cinco pares de juicios contradictorios.

3. Indicar cuáles de los pares de las proposiciones dadas en la respuesta al Ejercicio 1, son contradictorios.

4. El método de prueba por eliminación consiste en considerar todas las posibilidades y en eliminar todas ellas excepto una. Por ejemplo, si deseamos demostrar que el triángulo ABC es un triángulo isósceles rectángulo, habrá que considerar las siguientes posibilidades: (a) el triángulo ABC no es un triángulo rectángulo; (b) el triángulo ABC no es un triángulo isósceles; (c) el triángulo ABC es un triángulo isósceles rectángulo. Proponer otro ejemplo de esta clase de razonamiento.

5. Demostrar que $\sqrt{5}$ es un número irracional.

6. Expresar 1.41414 . . . en forma de número racional.

7. Expresar 3.176176176 . . . en forma de número racional.

8. Proponer cinco números racionales algebraicos.

9. Proponer cinco números irracionales algebraicos.

10. Dar ejemplos de tres números que el lector crea que son trascendentes (la demostración sistemática de que un número dado es trascendente puede ser muy difícil).

11. Indicar la relación entre la clasificación de los números reales en racionales e irracionales y la clasificación de los números reales en decimales exactos, infinitos periódicos o infinitos no periódicos.

12. Demostrar la necesidad de ampliar nuestro sistema de números reales, dando ejemplos de cinco números algebraicos que no sean números reales.

13. Hacer un cuadro indicando las relaciones entre los números reales, algebraicos, trascendentes, racionales, irracionales y enteros.

14. Encontrar ecuaciones (con coeficientes enteros) que se satisfagan con cada uno de los siguientes números:

(a) $3 + \sqrt{2}$ (c) $\sqrt{10 - 2\sqrt{5}}$

(b) $\sqrt{3 + \sqrt{2}}$ (d) $\sqrt[5]{4 - \sqrt[3]{2}}$

¿Tienen estos ejercicios una respuesta única? Explicar.

15. Demostrar que

$$(a + b\sqrt[3]{c - d})/e$$

es un número algebraico donde a, b, c, d, y $e \neq 0$ son enteros.

I-11* LOS POSTULADOS DE LOS NUMEROS REALES.

Repetiremos, ahora, el procedimiento de definir operaciones y relaciones respecto de nuevos símbolos. Los nuevos símbolos se llamarán *cortaduras de Dedekind* o,

*El asterisco indica que esta sección (Cap. 1 - 11) puede omitirse sin perturbar la organización del texto.

simplemente, *cortaduras*. El postulado siguiente que se refiere a la existencia de números que corresponden a cortaduras, se denomina *postulado de Dedekind*.

Si dividimos el conjunto de todos los números racionales en dos subconjuntos L y R de tal manera que todo número racional pertenezca ya sea a L o a R, pero no a ambos, que ni L ni R sean conjuntos vacíos y que a perteneciente a L y b perteneciente a R impliquen la relación $a < b$, existe, entonces, un número c cortadura tal que a perteneciente a L implica $a \leqq c$ y b perteneciente a R implica que $c \leqq b$.

Este procedimiento para formar una cortadura puede aplicarse a cualquier conjunto de elementos en el cual se hayan definido las relaciones de orden. Nos referiremos principalmente a cortaduras $\{L, R\}$ en el conjunto de los números racionales. Si L comprende a todos los números racionales $x \leqq 3$, y R contiene todos los $x > 3$, entonces $c = 3$ y c pertenece a L. Si L contiene a todos los números $x < 5$ y R a todos $x \geqq 5$, entonces $c = 5$ y c se encuentra en R. Nótese que c es racional y en estos dos ejemplos pertenece a L o a R. Si L contiene a todos los números negativos x, y a todos los números no negativos x, tales que $x^2 < 2$, y si R contiene a todos los números positivos x tales que $x^2 > 2$, entonces todos los números racionales se encuentran en L o en R y $c = \sqrt{2}$ no pertenece ni a L ni a R (Cap. 1-10). En general, cuando los conjuntos L y R son subconjuntos del conjunto de los números racionales, el número cortadura c se encuentra en L o en R, si y sólo si c es racional. Se dice que una cortadura es *cerrada* si el número cortadura c es un elemento del conjunto y, en caso contrario, la cortadura es *abierta*. Por eso, una cortadura en el conjunto de los números racionales es cerrada si c es racional, y abierta si c es irracional, es decir, no racional. El conjunto de todos los números cortaduras que se obtienen de cortaduras en el conjunto de los números racionales, se llama el conjunto de los *números reales*. El resultado de efectuar una cortadura en el conjunto de los números reales se acostumbra a enunciarlo en forma de un teorema, el *Teorema de Dedekind: Toda cortadura en el sistema de números reales es cerrada* (Ejercicio 10).

Dadas dos cortaduras $\{L, R\}$ y $\{S, T\}$ en el conjunto de los números racionales, formularemos las siguientes definiciones:

(i) $\{L, R\} = \{S, T\}$ si hay, a lo sumo, un elemento de S que no es elemento de L y viceversa, si hay, a lo sumo, un elemento de L que no es elemento de S.

(ii) $\{L, R\} < \{S, T\}$, si hay, por lo menos, dos elementos de S que no son elementos de L.

(iii) $\{L, R\} + \{S, T\} = \{U, V\}$, en donde U comprende a todos los números racionales que puedan expresarse en la forma $a + s$, donde a pertenece a L y s pertenece a S.

Las expresiones "a lo sumo un elemento" en (i) y "por lo menos dos elementos" en (ii), son necesarias, puesto que la cortadura $\{L, R\}$ donde L comprende a todos los $x < 2$ y la cortadura $\{S, T\}$ donde S contiene a todos los $x \geqq 2$ tienen el mismo número cortadura $c = 2$ y deben considerarse iguales. Cada una de las definiciones anteriores puede expresarse también (Ejercicio 4) con respecto a las condiciones de R, T y V, ya que por definición de una cortadura $\{L, R\}$ en el conjunto de los números racionales, todo número racional debe pertenecer a L o a R, de donde R contiene a todos los números racionales que no pertenecen a L.

La cortadura $\{N, P\}$ en la que todos los números racionales negativos y cero se encuentran en N y todos los números racionales positivos pertenecen a P, se denomina *cortadura cero*. Se dice que una cortadura $\{L, R\}$ es *negativa* si $\{L, R\} < \{N, P\}$; es *cero* si $\{L, R\} = \{N, P\}$ y es *positiva* si $\{N, P\} < \{L, R\}$. Una cortadura que es positiva o cero se dice que es *no negativa*. El producto de dos cortaduras $\{L, R\} \cdot \{S, T\} = \{U, V\}$ puede definirse considerando los casos posibles de cortaduras negativas y no negativas. Definiremos a V como el conjunto de números racionales que se pueden expresar en la forma as, donde a pertenece a L, y s pertenece a S, cuando las dos cortaduras dadas son negativas; y cuando las dos cortaduras dadas son no negativas, definiremos a V como el conjunto de números racionales que se expresa en la forma rt, donde r pertenece a R y t pertenece a T. Si una de las cortaduras dadas es no negativa y la otra es negativa, U comprende al conjunto de los números racionales que se expresan en la forma at, donde a pertenece a L y t pertenece a T, cuando $\{L, R\}$ es negativa; y cuando $\{S, T\}$ es negativa, U comprende al conjunto de los números racionales susceptibles de expresarse en la forma sr, donde s pertenece a S y r pertenece a R.

Ya hemos definido la igualdad, las relaciones de orden, la suma y la multiplicación para los nuevos símbolos $\{L, R\}$. Como en el caso de los símbolos a/b y $[a - b]$, queda por demostrar que existe un isomorfismo de orden entre un subconjunto de los nuevos símbolos y el conjunto dado de números, o sea, el conjunto de los números racionales. Consideraremos la correspondencia de $\{L, R\}$ con c, donde c es un número racional y L contiene a todos los números racionales $x \leqq c$. Esto es, en esencia, la correspondencia entre cortaduras cerradas y los números racionales, ya que V comprende a todos los números racionales $\leqq c$, luego $\{U, V\} = \{L, R\}$.

Dadas dos cortaduras $\{L, R\}$, $\{S, T\}$, que correspondan a números racionales a y b, respectivamente, las definiciones anteriores pueden aprovecharse para demostrar que $\{L, R\} = \{S, T\}$ si y sólo si $a = b$; que $\{L, R\} < \{S, T\}$, si y sólo si $a < b$; que $\{L, R\} + \{S, T\}$ corresponde a $a + b$; y que $\{L, R\} \cdot \{S, T\}$ corresponde a $a \cdot b$. Las demostraciones no son difíciles y se han dejado como ejercicio para el lector (Ejercicio 7). El isomorfismo de orden entre el conjunto de cortaduras cerradas y el conjunto de números racionales, muestra que para el conjunto de cortaduras cerradas, las definiciones anteriores son consistentes con nuestras definiciones previas. Tal como se señaló anteriormente, los números cortaduras representados por los nuevos símbolos se llaman números reales para cortaduras arbitrarias $\{L, R\}$ pertenecientes al conjunto de los números racionales. De esta manera, hemos obtenido números nuevos, *los números irracionales* que son los que corresponden a cortaduras abiertas. El Postulado de Dedekind sobre la existencia de un número cortadura c para todas las cortaduras pertenecientes al conjunto de los números racionales, sirve para postular la existencia de todos los números reales, racionales e irracionales en relación con los números racionales. El Teorema de Dedekind (todas las cortaduras en el conjunto de los números reales son cerradas) puede probarse (Ejercicio 10) demostrando que todas las cortaduras en el conjunto de los números reales determinan una cortadura en el conjunto de los números racionales. Varias otras propiedades de las cortaduras de Dedekind y de los números reales se tratarán en los ejercicios siguientes y en el Cap. 1-12.

EJERCICIOS

1. Citar dos ejemplos de cortaduras abiertas en el conjunto de números racionales.

2. Citar dos ejemplos de cortaduras cerradas en el conjunto de los números racionales.

3. Demostrar que toda cortadura en el conjunto de los números enteros es cerrada.

4. Formular de nuevo las definiciones anteriores (i) (ii) y (iii) con respecto a R, T, y V.

5. Proponer una cortadura cero $\{N', P'\} = \{N, P\}$ tal que los conjuntos N' y N sean diferentes.

6. Construir la cortadura que sea la suma de las dos cortaduras dadas en la respuesta del Ejercicio 1.

7. Dadas dos cortaduras cerradas $\{L, R\}$, $\{S, T\}$ correspondientes a a y b respectivamente, demostrar que $\{L, R\} = \{S, T\}$ si y sólo si $a = b$; $\{L, R\} < \{S, T\}$ si y sólo si $a < b$; $\{L, R\} + \{S, T\}$ corresponde a $a + b$; y $\{L, R\} \cdot \{S, T\}$ corresponde a $a \cdot b$.

8. Repetir el Ejercicio 6 respecto del producto.

9. Definir la sustracción de las cortaduras y repetir el Ejercicio 6 respecto de la sustracción.

10. Demostrar el Teorema de Dedekind.

11. Definir la división de una cortadura arbitraria por una cortadura diferente de cero. Dar un ejemplo numérico.

12. Demostrar que los números reales están ordenados linealmente (Cap. 1 — 6).

13. Demostrar que los números reales son densos (Cap. 1 — 8).

I-12 PROPIEDADES DE LOS NUMEROS REALES. Acabamos de aceptar que los números reales existen y están ordenados linealmente (Ejercicio 12, Cap. 1-11). Se los puede considerar ya sea como decimales (Cap. 1-10) o bien como cortaduras de Dedekind (Cap. 1-11). También damos por aceptado que se han definido las cuatros operaciones racionales y que tienen las mismas propiedades en el conjunto de los números reales que en el conjunto de los números racionales (Cap. 1-11).

Dado cualquier número real a y cualquier entero positivo b, determinaremos que el símbolo a^b representa el producto de b factores a. Si $a \neq 0$, definiremos $a^0 = 1$ y $a^{-b}\, a^b = 1$ para cualquier entero b. Si $a = 0$ y b es cualquier número real positivo, entonces

$a^b = 0$. Definiremos $(a^{1/b})^b = a$ para cualquier número racional b cuando $a > 0$, y para cualquier entero impar b cuando $a < 0$. Estas definiciones permiten conservar la propiedad $a^b\ a^c = a^{b+c}$ siempre que los símbolos estén definidos. En general, para cualquier número real a y para cualquier número racional b, por ejemplo, $b = r/s$ donde los enteros r, s no tienen factores comunes, el símbolo a^b representa un número real si y sólo si el entero r puede elegirse de modo que a^r esté definido y que la ecuación $x^s = a^r$ tenga una solución en el conjunto de los números reales. Este concepto puede aplicarse (Ejercicios 10, 11, 12 y 13) a los números reales a con el objeto de dar un significado preciso al símbolo a^b en el conjunto de los números reales sujetos a cualquiera de las siguientes condiciones:

(i) $a = 0$ y b es cualquier número positivo real;
(ii) $a > 0$ y b es cualquier número real, y
(iii) $a < 0$ y $b = r/s$ donde los enteros r, s no tienen factores comunes y s es número impar (no tiene factor 2).

Cuando $a = 0$ y $b \leqq 0$, no se le puede atribuir al símbolo a^b un significado explícito dentro del conjunto de los números reales y conservar, al mismo tiempo, la propiedad $a^b\ a^c = a^{b+c}$. Cuando $a < 0$ y b es irracional, o $b = r/s$, donde r y s no tienen factores comunes y s es par, el símbolo a^b no tiene un significado explícito en el conjunto de los números reales, pero puede definirse en el conjunto de los números complejos (Cap. I-16).

Todas las propiedades del conjunto de los números reales pueden considerarse también como propiedades del conjunto de puntos de una recta. Supondremos que el lector está familiarizado con el uso de un sistema de coordenadas cartesianas ortogonales en la geometría plana de Euclides. En cualquier sistema dado de coordenadas, como el ya citado, definiremos los puntos que tienen números enteros por coordenadas, como *puntos enteros;* definiremos como *puntos racionales* a los que tienen números racionales por coordenadas y como *puntos reales* a aquéllos que tienen por coordenadas, números reales. Dado un origen y un punto unidad, todos los puntos enteros y racionales pueden construirse con regla y compás (Cap. VI-4). También, pueden construirse algunos puntos irracionales, como $\sqrt{2}$, la diagonal de un cuadrado, cuyo lado es la unidad. La existencia del conjunto de los puntos irra-

cionales debe postularse. Euclides supuso que cualquier segmento de recta que uniera el centro de un círculo con un punto fuera del círculo, contenía un punto del círculo. Nosotros admitiremos el Axioma de *Cantor-Dedekind:*

A cada punto de una recta corresponde uno y sólo un número real e inversamente, a cada número real corresponde uno y sólo un punto de una recta.

Esta correspondencia biunívoca puede elegirse, como en el caso de los sistemas de coordenadas corrientes de modo que exista un isomorfismo de orden entre el conjunto de los puntos de la línea recta y el conjunto de los números reales. Esta correspondencia, pues, hace posible obtener una representación geométrica de las propiedades del conjunto de los números reales. Por ejemplo, los números reales y racionales son densos (Cap. 1-8); los enteros no son densos. Todos los números enteros, racionales y reales están ordenados linealmente (Cap. 1-6).

La propiedad que distingue al conjunto de los números racionales del conjunto de los números reales es la continuidad. Esta es la propiedad que se utiliza en geometría plana para demostrar que cualquiera recta que una el centro de un círculo con un punto fuera de él, debe cortar al círculo, por lo menos en un punto. Intuitivamente, una línea recta o curva es continua si no "se rompe" o "interrumpe". Técnicamente, valiéndonos del Axioma de Cantor-Dedekind, representaremos los elementos de cualquier conjunto dado ordenado linealmente como un conjunto ordenado de puntos de una recta, y consideraremos a los números reales (coordenadas) asociados con estos puntos. Definiremos entonces el conjunto de elementos dado ordenado linealmente y el conjunto de puntos asociado con él como *continuos* si y sólo si el conjunto correspondiente de números reales incluye a todos los números reales x o comprende a todos los números reales x que satisfacen alguna de las relaciones $a < x$, $x < b$, $a < x < b$ para algunos números reales a, b. Esta definición puede formularse en forma mucho más elegante empleando la terminología del Cap. 1-11. Se dice que un conjunto de elementos linealmente ordenados, es continuo, si es denso y satisface el Postulado de Dedekind. Es así como los números racionales son densos, pero no continuos; los números rea-

les son densos y continuos. Las definiciones anteriores de conjuntos densos y continuos pueden ampliarse a conjuntos de puntos en un plano y a muchos otros conjuntos que no pueden ser ordenados linealmente.

Las proposiciones contenidas en el Ejercicio 9 señalan, principalmente, métodos para ampliar un conjunto denso, ordenado linealmente y convertirlo en un conjunto continuo. Por ejemplo, cada uno de los números.

$$1,\ 1.4,\ 1.41,\ 1.414,\ 1.4142,\ 1.41421,\ 1.414214,\ \ldots$$

puede expresarse en forma de un número racional que tenga por denominador una potencia de diez (Cap. I-10). Sin embargo, si consideramos una sucesión tal de números $x_1, x_2, x_3, \ldots$, que satisfaga,

$$2 - x_1^2 > 2 - x_2^2 > 2 - x_3^2 > \ldots,$$

y tal que para cualquier número *e racional* positivo dado, el número positivo $2 - x_n^2$ pueda hacerse menor que e eligiendo n suficientemente grande, es decir, haciendo aproximaciones más y más próximas a $\sqrt{2}$, entonces esta sucesión sin fin de números puede decirse que define un nuevo número $\sqrt{2}$. En la terminología del análisis algebraico, la sucesión anterior de números racionales tiene a $\sqrt{2}$ como límite (Cap. III-11). En general, cualquier conjunto de elementos denso ordenado linealmente puede hacerse continuo agregando todos los límites de las sucesiones convergentes de sus elementos (Cap. III-11). Por ejemplo, el conjunto de los números racionales se convirtió en un conjunto continuo (el conjunto de los números reales) al agregar los números irracionales. Todo número irracional puede expresarse como límite de una sucesión de números racionales.

La última propiedad de los números reales que consideraremos es la propiedad de tener límites. La palabra "límite" se usa frecuentemente para indicar un ámbito que no puede o no debe excederse. La frase "fuera de los límites" es corriente en muchos juegos. Todo objeto físico tiene límites. Las inmensas regiones polares despobladas de la Antártica están limitadas por océanos. El aire

que respiramos es una parte de la atmósfera de la tierra que está limitada, dado que no se extiende hasta el sol, hasta otro planeta, ni aún hasta la luna. El número de pelos de la cabeza de una persona y el número de granos de arena de la playa de Miami son limitados, aun cuando, por lo menos, en el segundo caso, el número es grande.

La palabra "ilimitado" se usa para indicar que un objeto o los elementos de un conjunto exceden cualquier límite que se pretenda establecer para él. Se dice que el conjunto de enteros positivos es ilimitado, ya que si se considera cualquier número real M como límite, siempre existe un número entero n tal que $n > M$. Para ser más exactos, decimos que los enteros positivos tienen un límite inferior que es cero, o cualquier número negativo y que en su extremo superior son ilimitados. Lo mismo puede decirse de los números reales positivos. Los enteros negativos son ilimitados en su extremo inferior y son limitados en su extremo superior. El conjunto de todos los enteros es ilimitado en sus extremos inferior y superior, es decir, es *ilimitado*. Análogamente, los números reales son ilimitados.

El conjunto de los números reales positivos $\leqq N$ está limitado por 0 y por N. Cualquier conjunto numerado de números reales está limitado. Por ejemplo, el conjunto 1, 5, 75, 32, 17, -4 está limitado por -4 y 75 o por -10 y 100, ... En efecto, los límites no son únicos y cualquier número real determinado está limitado. Por ejemplo, cualquier número real n está limitado por $n - 1$ y $n + 1$. Cada uno de los números reales, considerados individualmente, está limitado, pero el conjunto de todos los números reales es ilimitado. Lo mismo puede decirse del conjunto de números enteros. Se dice que un conjunto de números reales está *limitado* si existe un número entero positivo fijo N tal que $-N < b < N$ para todos los elementos b del conjunto. En la sección siguiente de este capítulo consideraremos conjuntos ilimitados de elementos y nos referiremos, particularmente, a los conjuntos de elementos que puedan ordenarse en correspondencia biunívoca con respecto al conjunto de los números enteros positivos.

EJERCICIOS

1. Indicar cuáles de los siguientes conjuntos de elementos son linealmente ordenados: (a) los números enteros; (b) los números racionales; (c) los nú-

meros irracionales; (d) los números reales algebraicos; (e) los puntos de un círculo en la geometría de Euclides, y (f) los puntos de un segmento de recta limitado en la geometría de Euclides.

2. Señalar cuáles de los conjuntos de elementos del Ejercicio 1 son densos.

3. Indicar cuáles de los conjuntos de elementos del Ejercicio 1 son continuos.

4. Demostrar que todo conjunto continuo linealmente ordenado, debe ser también denso.

5. Indicar una propiedad del conjunto de los números reales que lo distinga del conjunto de los números racionales.

6. Indicar una propiedad del conjunto de los números racionales que lo distinga del conjunto de los números enteros.

7. Citar tres conjuntos de números que posean las siguientes propiedades: (a) tener límite inferior y superior; (b) tener límite inferior solamente; (c) tener límite superior solamente; (d) ser ilimitados; (e) ser limitados.

8. Citar dos conjuntos de límites, en el caso de que exista alguno, para cada uno de los conjuntos de números dados en las respuestas al Ejercicio 7.

9. Dar ejemplos algebraicos o geométricos de cada una de las siguientes proposiciones. Cada proposición puede servir para postular la existencia del conjunto de números reales y, en este sentido, es equivalente al Postulado de Dedekind. Cualquiera de estas proposiciones puede considerarse también como base suficiente para probar la continuidad tanto en álgebra como en geometría.

a) Toda fracción decimal está dada como un número real.

b) *Teorema de Bolzano Weierstrass:* Todo conjunto acotado de infinitos puntos admite por lo menos un punto límite.

c) Todo conjunto de puntos acotado en su extremo inferior tiene una cota inferior máxima.

d) Todo conjunto de puntos acotado en su extremo superior tiene una cota superior mínima.

e) *Teorema de Heine - Borel - Lebesgue:* Si un conjunto infinito de intervalos I comprende un conjunto fundamental de puntos S en un intervalo cerrado finito, entonces, existe un subconjunto finito de I que comprende a S.

f) Toda sucesión de Cauchy de números racionales determina un número real (Cap. III-11).

g) *Teorema de Cantor:* Dada una sucesión cualquiera de intervalos E_1, E_2, E_3, ..., sobre una recta, en que E_i está determinado por $a_i \leqq x \leqq b_i$ y en donde se verifican las relaciones $a_1 \leqq a_2 \leqq a_3 \leqq \cdots, \cdots \leqq b_3 \leqq b_2 \leqq b_1$, entonces existe por lo menos un punto, sea $x = x_0$, que pertenece a todos los intervalos de la sucesión.

10. Definir a^b para cualquier número real $a \neq 0$ y para cualquier entero b.

*11. Definir a^b como un número positivo para cualquier número real positivo a y cualquier número real b.

12. Definir a^b para cualquier número real negativo a y cualquier número racional $b = r/s$, donde los enteros r, s no tengan factores comunes y s sea impar.

13. Demostrar que a^b está determinado unívocamente por las condiciones expuestas en los Ejercicios 10, 11, 12.

I-13 LOS NUMEROS CARDINALES TRANSFINITOS. En las secciones 1 y 2 del Cap. 1 se han considerado los números cardinales asociados con conjuntos finitos de elementos. Dos conjuntos finitos tienen el mismo número cardinal si y sólo si existe una correspondencia biunívoca entre los elementos de los dos conjuntos. Ahora, mediante correspondencias biunívocas, asociaremos números cardinales (*números cardinales transfinitos*) con conjuntos infinitos (Cap. 1-2).

Dos conjuntos infinitos de elementos tienen el mismo número cardinal transfinito si y sólo si existe una correspondencia biunívoca entre los elementos de los dos conjuntos. Como en el caso de los conjuntos finitos, se dice que dos conjuntos infinitos que tienen el mismo número cardinal son equivalentes. Sin embargo, un conjunto infinito puede ser equivalente a uno de sus propios subconjuntos. Por ejemplo, el conjunto de los enteros positivos n es equivalente al conjunto de los enteros positivos pares según se desprende de la correspondencia de n con $2n$. Debido a esta propiedad de los conjuntos infinitos, una correspondencia biunívoca entre los elementos del conjunto A y de un subconjunto propio de un conjunto B, significa solamente que el número cardinal del conjunto A es menor que o igual al número cardinal del conjunto B. Con el objeto de demostrar que el número cardinal de un conjunto A es menor que el número cardinal de un conjunto B, es necesario probar que A es equivalente a un subconjunto propio de B y que no existe una correspondencia biunívoca entre los elementos de A y los elementos de B.

Si un conjunto de elementos tiene un número cardinal tres, sus elementos pueden ordenarse en correspondencia biunívoca con el conjunto 1, 2, 3, de los enteros positivos. Si un conjunto está repre-

*Para la solución de este ejercicio se requiere la materia presentada en el Cap. 1-11

sentado por un número cardinal n, sus elementos pueden ordenarse en correspondencia biunívoca con el conjunto 1, 2, 3 ... n, de enteros positivos. Si los elementos de un conjunto pueden ordenarse en correspondencia biunívoca con el conjunto de todos los enteros positivos 1, 2, 3, ..., su número cardinal se llama *Aleph-cero*, $\aleph_0$ y se dice que el conjunto es *infinito contable* o *infinito numerable*. El conjunto de todos los enteros positivos.

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \ldots \qquad n \qquad ,$$

el conjunto de los enteros positivos pares

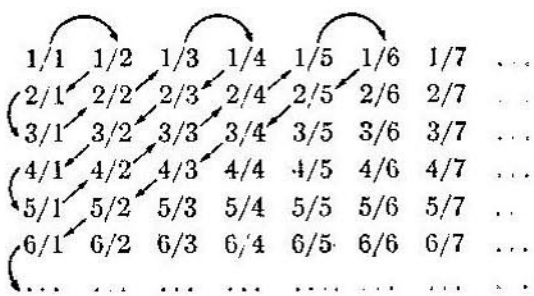
$$2 \quad 4 \quad 6 \quad 8 \ 10 \ 12 \ 14 \ldots \qquad 2n \qquad \ldots,$$

el conjunto de los enteros positivos impares

$$1 \quad 3 \quad 5 \quad 7 \quad 9 \ 11 \ 13 \ldots \qquad 2n-1 \ \ldots,$$

y aún el conjunto de los números racionales positivos, como lo demostraremos más adelante, son infinitos numerables.

El conjunto de los números racionales positivos es por lo menos infinito numerable, pues tiene como subconjunto al conjunto de los números enteros positivos. Demostraremos que el conjunto de los números racionales positivos es a lo sumo infinito numerable demostrando que el conjunto de todos los pares de enteros positivos es infinito numerable. Consideremos el cuadro



y asociemos un entero positivo con cada par siguiendo la dirección de las líneas diagonales tal como se indica en el cuadro:

$$1 \sim 1/1, \quad 2 \sim 1/2, \quad 3 \sim 2/1, \quad 4 \sim 3/1, \quad 5 \sim 2/2, \ldots$$

Esta correspondencia biunívoca entre el conjunto de los enteros positivos y el conjunto de todos los pares de enteros positivos indica que el conjunto de pares es infinito numerable. Dado que el conjunto de números racionales positivos es un subconjunto del conjunto de todos los pares de números enteros positivos, el conjunto de números racionales positivos no es superior a infinito numerable. Luego, ya que es también por lo menos infinito numerable, el conjunto de los números racionales positivos es infinito numerable.

La correspondencia anterior entre los números racionales positivos y los enteros positivos proporciona una ordenación de los números racionales positivos. Esta ordenación satisface las condiciones de un conjunto ordenado linealmente (Cap. 1 - 6), pero evidentemente no es una ordenación conforme a la magnitud o medida de los números. Por ejemplo, según este orden, 2 precede a 1/4 y a 3.

Dado que el conjunto de los múltiplos de mil, el conjunto de los números enteros pares, el conjunto de los números enteros impares, el conjunto de los números enteros, y el conjunto de los números racionales tienen todos el mismo número cardinal, surge la cuestión de que si todos los conjuntos infinitos de números reales son infinitos numerables. Puede demostrarse que el conjunto de los números reales algebraicos es infinito numerable (Ejercicio 5) y que el conjunto de los números reales trascendentes no es infinito numerable (Ejercicio 6).

Si se representan únicamente los puntos enteros por medio de puntos sobre una recta, es fácil ver los "saltos" en la recta. Una vez que se han agregado todos los puntos racionales, los puntos se presentan densos y sin embargo, si se considera la recta como el eje de las x, y se describe el círculo con centro en el origen y radio $\sqrt{2}$, este círculo corta la recta sin encontrarse con ningún punto racional, de modo que debe haber aún "saltos" en la recta. Si se agregaran aún todos los puntos cuyas abscisas son números reales algebraicos (Cap. 1 - 10), todavía habría "saltos" ya que si la circunferencia de un círculo de radio igual a la unidad, pudiera cortarse, estirarse en línea recta colocando un extremo en el origen, el otro

extremo llegaría al punto trascendente 2π. Cuando se han representado todos los números reales no hay ningún "salto" en la recta.

Consideremos el conjunto de los números reales entre cero y uno y representémoslos como números decimales. Si el conjunto es infinito numerable, los decimales pueden ordenarse en correspondencia biunívoca con los enteros positivos y pueden escribirse en lista en el orden impuesto por esta correspondencia. Supongamos que el orden impuesto es

.1284 . . .
.2315 . . .
.1694 . . .
.7850 . . .
. . . . . .
. . . . . .

De acuerdo con la suposición de que el conjunto es infinito numerable, todos los decimales entre cero y uno se encuentran en el esquema anterior. Supongamos que formamos un decimal tomando los elementos .1390 . . . de la diagonal principal y aumentamos cada elemento en 1, excepto el 9 que se reemplaza por 0. El nuevo decimal en este caso es .2401 . . . y se encuentra entre el cero y el 1. Este decimal no se encuentra en la primera fila, ya que sus primeros elementos difieren; no está en la segunda fila, ya que sus segundos elementos difieren; y en general, no está en la j-ésima fila, puesto que los j-ésimos elementos difieren. De aquí que el decimal formado no se encuentre en el esquema, y que la suposición de que los números reales entre cero y uno son numerables nos ha conducido a una contradicción. En resumen, si el conjunto de los números reales entre cero y uno es infinito numerable, los números reales de ese conjunto pueden ponerse en una lista en algún orden como se hizo más arriba. Cualquiera que sea este orden, podríamos, si fuese necesario, volver a ordenar los números de modo que por lo menos uno de los dígitos de la diagonal principal no sea 8 sino 9 y, por medio de este procedimiento, formaríamos un nuevo decimal que no se encuentre en la lista. Por consiguiente, los números reales entre cero y uno no pueden ponerse en lista en ningún orden y el conjunto no es infinito numerable. Por esta razón el conjunto de los números reales es infinito, pero no infinito numerable, ya que uno de sus subconjuntos es infinito y no infinito numerable.

El número cardinal asociado con el conjunto de todos los números reales se llama el *número cardinal del continuo C*. El infinito numerable $\aleph_0$ es el primero, o sea el número cardinal transfinito menor. Uno de los problemas matemáticos famosos no resueltos es demostrar que C es el número transfinito siguiente a $\aleph_0$, es decir, $C = \aleph_1$. Hay por lo menos un conjunto infinito numerable de números cardinales transfinitos diferentes (ver Bibliografía Nº 13, págs. 84-85; y Nº 29, págs. 54-55), pero los dos anteriores son los más comunes.

La correspondencia entre los números reales y los puntos sobre una recta en la geometría euclidiana corriente, es válida sólo para números finitos. Los números transfinitos no se incluyen en el conjunto de los números reales y tienen relaciones completamente diferentes de las de los números reales. Por ejemplo, $\aleph_0 \pm a = \aleph_0$, donde a es igual a $\aleph_0$ o a cualquier número cardinal finito; $\aleph_0 + C = C$; $\aleph_0 \cdot 5 = \aleph_0$.

EJERCICIOS

1. Dar tres ejemplos de cada uno de los siguientes ejercicios: (a) un conjunto finito y un subconjunto finito propio; (b) un conjunto infinito y un subconjunto finito; (c) un conjunto infinito y un subconjunto infinito propio; (d) un conjunto infinito numerable; (e) un conjunto infinito que no sea infinito numerable.

2. Demostrar que los números racionales negativos son infinitos numerables.

3. Demostrar que cualquiera función $f(x)$ definida (Cap. III-10) para valores enteros positivos de x, toma una sucesión infinita numerable de valores (no necesariamente distintos) a medida que x toma los valores 1, 2, 3, ...

4. Dar tres ejemplos de sucesiones de números obtenidas como se señala en el Ejercicio 3.

5. Demostrar que el conjunto de los números reales algebraicos es infinito numerable (ver Bibliografía Nº 13; pág. 103).

6. Demostrar que el conjunto de números reales trascendentes no es infinito numerable

I-14 GRUPO; SISTEMA DE NUMEROS.

Hemos estudiado el sistema de números racionales y el sistema de los números reales. En esta sección estudiaremos el concepto de

grupo y estableceremos con toda exactitud qué se entiende por un "sistema de números".

Un conjunto de elementos forma *un grupo* con respecto a una operación $\oplus$ binaria única cualquiera (Cap. 1 - 2) si ella es: (1) cerrada (2) asociativa; y contiene (3) un elemento de identidad; y (4) el inverso de cada uno de sus elementos. En otras palabras, el conjunto C de elementos $a, b, \ldots$ forma un grupo con respecto $a \oplus$ *si* (1) $a \oplus b$ está en C para todos los pares a, b de C; (2) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ para todo a, b, c, de C; (3) hay un elemento I de C tal que $I \oplus a = a \oplus I = a$ para todo elemento a de C; y (4) para todo a de C hay un elemento a' en C tal que $a \oplus a' = a' \oplus a = I$. Por ejemplo, el conjunto de los enteros (positivos, negativos y cero) forma un grupo con respecto a la operación de la adición pero no con respecto de la operación de la multiplicación. El conjunto de los números racionales (y también el conjunto de los números reales) forma un grupo con respecto a la adición. Si se excluye el cero, los números racionales restantes forman un grupo con respecto a la multiplicación.

Se dice que un grupo es *conmutativo* (o Abeliano) si $a \oplus b = b \oplus a$ para todos los elementos a, b, del grupo.

Un conjunto de elementos en el cual están definidas dos operaciones binarias $+$ y $\times$ forma un *sistema de números* o *campo conmutativo* si: (1) el conjunto forma un grupo conmutativo con respecto $a +$; (2) el conjunto, sin el elemento de identidad para $+$, forma un grupo con respecto a $\times$; y (3) las leyes de la distributividad de $\times$ con respecto a $+$,

$$a \times (b + c) = a \times b + a \times c, \quad (b + c) \times a = b \times a + c \times a,$$

son válidas para tres elementos cualesquiera a, b, c del conjunto. Un sistema de números en el cual la $\times$ es conmutativa se llama *campo**.

Si a y b son elementos de un sistema de números tal que $ab = 0$ y $a \neq 0$, entonces existe a^{-1} de acuerdo con (2), $a^{-1}ab = 0$, y $b = 0$. En otras palabras, si el producto de dos elementos de un sistema de números es cero, entonces por lo menos uno de los elementos debe ser cero. En rigor, un elemento $k \neq 0$ se llama un *divisor cero*

*Los autores franceses emplean el término "cuerpo". (N. de la T.).

si existe un elemento $j \neq 0$ tal que $j \cdot k = 0$ (ver Ejercicio 13, Cap. II - 9). La demostración anterior prueba que los divisores cero no pueden existir en un sistema de números.

Si un sistema de números contiene a los enteros positivos, debe contener también (i) a cero y a los enteros negativos, es decir, al elemento de identidad y a los inversos aditivos; y (ii) a los números racionales, ya que debe incluir a los inversos respecto a la multiplicación de todos los enteros diferentes de cero y a todas las sumas finitas de estos inversos. Por consiguiente, cualquier sistema de números que contiene a los enteros positivos debe contener a los números racionales. Los números racionales, los números reales, y —como veremos pronto— los números complejos, forman sistemas de números. Los conjuntos de los números racionales, reales y complejos forman también sendos campos, dado que hemos determinado que la adición y la multiplicación son operaciones conmutativas.

La definición exacta que hemos dado de un sistema de números contiene los conceptos básicos de este término matemático corriente. Es aún de mayor importancia fundamental la introducción de los conceptos de grupo y de campo que junto con el concepto de anillo (Cap. I - 18) forman la base de la mayoría de las definiciones del álgebra abstracta.

EJERCICIOS

1. Indicar cuáles de los conjuntos de números siguientes forman grupos respecto a la adición.

a) números enteros pares,

b) números enteros impares,

c) múltiplos enteros de diez,

d) múltiplos enteros de cualquier entero k,

e) enteros positivos,

f) números de la forma $b\sqrt{2}$ en que b es un número racional,

g) números de la forma $a + b\sqrt{2}$, en que a y b son enteros,

h) números de la forma $a + b\sqrt{2}$, en que a y b son números racionales,

i) 0,

j) números racionales positivos,

k) números irracionales,

l) números de la forma $a + bw$, donde a y b son números racionales cualesquiera y w es un número algebraico dado (Cap. I-18).

2. En cada uno de los conjuntos de números del Ejercicio 1, excluir el cero cada vez que se presente e indicar cuáles de los conjuntos de números que resultan forman grupos respecto a la multiplicación.

3. Demostrar que si en un conjunto de elementos la adición es asociativa, el conjunto es cerrado respecto a la sustracción y que este conjunto forma un grupo respecto a la adición.

1-15 LOS NUMEROS COMPLEJOS.

Hemos comenzado por los números enteros positivos, desarrollamos en seguida el sistema de números racionales con el fin de obtener un conjunto de números que sea cerrado para las cuatro operaciones racionales (adición, multiplicación, sustracción, división) e introdujimos el sistema de números reales para obtener un conjunto de números en el cual puedan representarse todas las magnitudes finitas. En los sistemas de números racionales y reales, las relaciones de orden e igualdad, así como las operaciones de adición y multiplicación tienen las mismas propiedades básicas que en el conjunto de los números enteros (Cap. 1-5 y Cap. 1-6). En esta sección repetiremos una vez más el procedimiento para definir las relaciones y operaciones para un nuevo símbolo, probando con respecto a un subconjunto de los símbolos, que estas definiciones son consistentes con las definiciones anteriores y definiendo los nuevos símbolos como números. Todos los símbolos finitos considerados anteriormente para los números podían ser representados como puntos sobre una recta en la geometría plana corriente y estaban linealmente ordenados. Los nuevos símbolos que consideraremos ahora deberán representarse sobre un plano en vez de sobre una recta en la geometría plana corriente. Por consiguiente, los nuevos símbolos no están ordenados linealmente y no consideraremos sus relaciones de orden.

Los nuevos símbolos que vamos a presentar son indispensables para resolver las ecuaciones algebraicas. Nuestro estudio anterior sobre los números algebraicos finitos puede considerarse desde otro punto de vista, a saber: encontrar números que correspondan a todas las raíces reales de una ecuación polinomia, es decir, números para designar los puntos en los cuales una curva polinómica corta el eje x en el plano real. Si a, b, c son enteros positivos arbitrarios, se necesitan los números racionales positivos para resolver todas las ecuaciones de la forma $ax = b$; a menudo se necesitan números

negativos para resolver ecuaciones de la forma $x + a = b$, y números reales (racionales y algunos irracionales) para resolver ecuaciones de la forma $ax^2 + bx + c = 0$ donde $b^2 - 4ac \geqq 0$. Todos los ceros de un polinomio $f(x)$ que *aparecen como intersecciones geométricas corrientes* del gráfico de $y = f(x)$ con el eje real x son, por supuesto, números reales. Sin embargo, algebraicamente conviene que la ecuación de segundo grado $x^2 + 2ax + b = 0$, tenga dos raíces, sea que la curva $y = x^2 + 2ax + b$ corte el eje x o no en la geometría plana de Euclides, es decir, para valores reales cualesquiera de a y b. En consecuencia, ampliaremos una vez más nuestro sistema de números para incluir un nuevo tipo de número.

Consideraremos ahora, pares ordenados de números reales (a, b) donde

$$\begin{aligned}
&\text{(i)} \quad (a, b) = (c, d) \text{ si y sólo si } a = c \text{ y } b = d;\\
&\text{(ii)} \quad (a, b) + (c, d) = (a + c, b + d);\\
&\text{(iii)} \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).
\end{aligned}$$

Como en el caso de otros símbolos nuevos, consideraremos una correspondencia entre un subconjunto $(a, 0)$ de los nuevos símbolos y el conjunto de los números reales a. También, como antes, las definiciones anteriores pueden usarse para demostrar que esta correspondencia es un isomorfismo (Ejercicio 1). Nótese que en este caso el isomorfismo no se denomina isomorfismo de orden.

Los nuevos símbolos (a, b) se definen como números, *números complejos*, para números reales cualesquiera a, b. El número a se llama la *parte real* del número complejo (a, b); b se llama la *parte imaginaria*. Se dice que el número complejo (a, b) es *imaginario* si $b \neq 0$, y que es *imaginario puro* si $b \neq 0$ y $a = 0$. Según el isomorfismo anterior el conjunto de los números complejos (a, b) comprende al conjunto de los números reales $(b = 0)$ y al conjunto de los números imaginarios $(b \neq 0)$. En vista de que los números complejos no están ordenados linealmente en cuanto a magnitud, la clasificación de números en positivos, cero y negativos se usa sólo para los números reales. De modo que los números negativos y positivos se refieren siempre a los números reales negativos y a los números reales positivos.

Ahora podremos demostrar que las raíces de $x^2 + 1 = 0$ son

$(0,1)$ y $(0, -1)$. Tenemos, en realidad $(0, 1)^2 = (0, 1) \cdot (0,1) = (0 - 1, 0 + 0) = (-1, 0) = -1$ y $(0, -1)^2 = (0, -1) \cdot (0, -1) = (0 - 1, 0 + 0) = (-1,0) = -1$. La manipulación mecánica de los números complejos se simplifica grandemente escribiendo $(0, 1) = i$. Entonces $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0,1 = a + bi$, y podemos considerar que a, b, i son números sujetos a la condición que $i^2 = -1$ todas las veces que aparezca i^2. Por consiguiente,

$$\begin{aligned}(2, 3)^3 = (2 + 3i)^3 &= 8 + 36i + 54i^2 + 27i^3 \\ &= 8 + 36i - 54 - 27i \\ &= -46 + 9i = (-46, 9).\end{aligned}$$

La palabra *complejo* denota que los nuevos números no son números simples, como se tenía entendido en el pasado, sino que cada uno es un par ordenado de números tales que satisfacen las condiciones (i) y (ii) anteriores. Es incorrecto emplear la palabra imaginario como opuesto a real. Excepto en el sentido técnico sobre el que están de acuerdo los matemáticos, las dos clases de números son igualmente reales.

Se puede considerar que los números negativos resultan de la rotación del eje positivo x en torno al origen en 180°. Si esta rotación se efectúa dos veces, se obtiene la identidad $-(-a) = a$. En este sentido, la multiplicación por -1 y la rotación en 180° son equivalentes (Fig. 1-2).

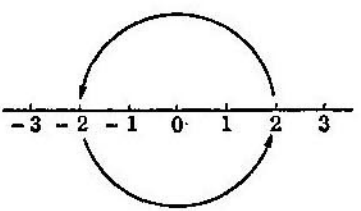


FIG. 1-2

De manera análoga, la multiplicación por i es equivalente a una rotación de 90°. Si la multiplicación o la rotación se aplica dos veces, se obtiene el número negativo y si se aplica cuatro veces, se obtiene el número original (Fig. 1-3).

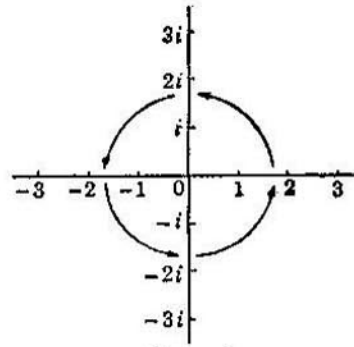


FIG. 1-3

Un plano tal como el de la Fig. 1 - 3 con un eje de números reales y un eje de los números imaginarios suele denominarse un *plano complejo*. Cada número complejo $a + bi = (a, b)$ puede asociarse con un punto único en el plano complejo con la coordenada a sobre el eje real y b sobre el eje imaginario (Cap. 1 - 16).

Los números complejos $a + bi$ y $a - bi$ son cada uno el *conjugado* del otro. La *norma* $n(z)$ de un número complejo z es el producto del número por su conjugado. Por eso si $z = a + bi$, $n(z) = n(a + bi) = (a + bi)(a - bi) = a^2 + b^2$, que para $z \neq 0$, es siempre positivo.

El *valor absoluto o módulo de* $z = a + bi$ es la raíz cuadrada no negativa de la norma $|z| = \sqrt{a^2 + b^2}$. De manera que el valor absoluto de un número complejo es siempre un número real.

Cuando buscamos el cuociente de dos números complejos $(a, b) \div (c, d)$, en realidad buscamos un número (p, q) tal que

$$(a, b) = (c, d) \cdot (p, q).$$

Tenemos

$$\begin{aligned}(a, b) &= (cp - dq, cq + dp),\\ a &= cp - dq,\\ b &= dp + cq,\end{aligned}$$

de donde

$$p = \frac{ac + bd}{c^2 + d^2}, \quad q = \frac{bc - ad}{c^2 + d^2}$$

si $c^2 + d^2 \neq 0$. Por consiguiente, de la unicidad de la suma, de la diferencia, del producto y del cuociente de los números reales, obte-

nemos números reales únicos p y q toda vez que $c^2 + d^2 \neq 0$, es decir, siempre que $(c, d) \neq 0$. Esto completa la demostración del teorema siguiente:

TEOREMA 1 - 1. *En el sistema de números complejos, la división es siempre posible y es única, con excepción de la división por cero.*

En la práctica, existe la costumbre de indicar la división de $z_1 = a + bi$ por $z_2 = c + di$ por medio del cuociente $z_1/z_2 = (a + bi) / (c + di)$. Este cuociente se expresa entonces como un número complejo multiplicando su numerador y su denominador por el conjugado de z_2, es decir,

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i.$$

En el Cap. 1 - 16 se estudian otras representaciones de z_1/z_2. En esa oportunidad trataremos también las relaciones entre los valores absolutos y los módulos de z_1 y z_2. En particular, necesitaremos demostrar que el valor absoluto de un producto de números complejos es igual al producto de los valores absolutos de sus factores. Este hecho es una consecuencia del Teorema 1 - 2, que formularemos y demostraremos en seguida.

TEOREMA 1 - 2. *La norma de un producto es igual al producto de las normas de sus factores.*

Sea $z_1 = a + bi$, $z_2 = c + di$, entonces $n(z_1) = a^2 + b^2$, $n(z_2) = c^2 + d^2$, $z_1z_2 = ac - bd + (ad + bc)i$, y además

$$\begin{aligned} n(z_1z_2) &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= n(z_1) \cdot n(z_2). \end{aligned}$$

Esto demuestra el teorema para el producto de dos factores. Dado que el producto de dos números complejos es también un número complejo, la demostración puede repetirse con $z_1 = w_1w_2$, $z_2 = w_3$

para demostrar el teorema para tres factores, y en general con $z_1 = w_1 w_2 \ldots w_{n-1}$ y $z_2 = w_n$ para demostrar el teorema para cualquier número finito de factores por inducción matemática (Cap. 1-4).

En el caso de la suma de los números complejos podemos demostrar

TEOREMA 1-3. *El valor absoluto de una suma de números complejos es menor que o igual a la suma de los valores absolutos.*

Supongamos $|z_1 + z_2| > |z_1| + |z_2|$ donde $z_1 = a + bi$, $z_2 = c + di$. Entonces

$$\sqrt{(a+c)^2 + (b+d)^2} > \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2},$$

de donde

$$\begin{aligned}
(a+c)^2 + (b+d)^2 &> a^2 + b^2 + 2\sqrt{(a^2+b^2)(c^2+d^2)} + c^2 + d^2, \\
a^2 + c^2 + b^2 + d^2 + 2ac + 2bd &> a^2 + b^2 + c^2 + d^2 + 2\sqrt{(a^2+b^2)(c^2+d^2)}, \\
ac + bd &> \sqrt{(a^2+b^2)(c^2+d^2)}, \\
a^2c^2 + b^2d^2 + 2abcd &> a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2, \\
0 &> b^2c^2 - 2abcd + a^2d^2, \\
0 &> (bc - ad)^2.
\end{aligned}$$

Pero esto es imposible, dado que el miembro de la derecha es el cuadrado de un número real y por lo tanto no negativo. De esta manera la suposición de que el teorema es falso ha conducido a una contradicción, y hemos hecho una demostración indirecta (Cap. 1-10) del teorema para la suma de dos números complejos. Esta demostración puede ampliarse por inducción matemática y aplicarse a cualquier suma finita de la misma manera que se amplió la demostración anterior referente a los productos.

EJERCICIOS

1. Demostrar que la correspondencia de $(a, 0)$ respecto de a es un isomorfismo.

2. Valiéndose de conocimientos adquiridos previamente, proponer una ecuación de segundo grado con coeficientes reales que tenga sus raíces en el conjunto de (a) los números enteros, (b) los números racionales, (c) de los números reales irracionales, (d) de los números imaginarios, (e) los números imaginarios puros.

3. Demostrar que los números complejos forman un sistema de números.

4. Expresar en la forma $a + bi$:

$$\sqrt{-16},\quad 5,\quad -\tfrac{2}{3},\quad 1+\sqrt{-2},\quad \frac{2+\sqrt{-3}}{2-\sqrt{-3}},\quad \frac{1}{3+4i}.$$

5. Determinar el módulo de cada uno de los números complejos dados en el Ejercicio 4.

6. Demostrar que si un número complejo es igual a su conjugado, el número es real.

7. Demostrar que si el producto de dos números complejos es cero, entonces por lo menos uno de los números es cero.

I-16 PROPIEDADES DE LOS NUMEROS COMPLEJOS. Las relaciones entre el álgebra y la geometría son importantes especialmente para aquellas personas que intentan aprender los conceptos fundamentales de matemáticas. Hemos visto en el (Cap. 1 - 12) que todos los números reales pueden representarse como puntos sobre una recta e inversamente, todos los puntos de una recta en la geometría de Euclides pueden representarse por números reales. En esta sección del Cap. 1 consideraremos dos representaciones de números complejos en un plano euclidiano. En seguida, de estas representaciones gráficas deduciremos representaciones trigonométricas y exponenciales para los números complejos.

Dado un sistema ortogonal de coordenadas cartesianas de origen 0 y ejes $0x$ y $0y$, tomamos a $0x$ como el eje de los números reales y a $0y$ como el eje de los números imaginarios. El número complejo $z = a + bi$ puede representarse ya sea por el punto P: (a, b) o bien, si $z \neq 0$ por el segmento de recta orientado, *vector*, **OP** (Fig. 1 - 4).

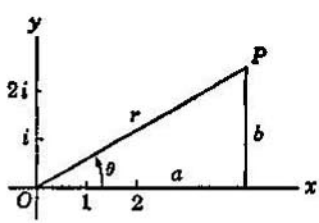


FIG 1-4

Un vector tiene longitud y dirección. La longitud r de **OP** está dada por el valor absoluto de z; su dirección está dada por el ángulo θ formado por el eje positivo x y **OP**. Para cada z, el número no negativo $r = \sqrt{a^2 + b^2}$ está determinado unívocamente, pero $\theta = arc\ tg\ b/a$, la *amplitud* o *argumento* de z, puede determinarse sólo dentro

de un múltiplo de 2π. El número complejo $z = a + bi$ y el punto $P{:}(a, b)$ están unívocamente determinados ya sea por el par de números reales (a, b), esto es, las coordenadas *ortogonales o cartesianas* del punto P, o por el par de números reales (r, θ), esto es, las *coordenadas polares* del punto P. Empleando funciones trigonométricas, $a = r\cos\theta$, $b = r\operatorname{sen}\theta$, y $z = r(\cos\theta + i\operatorname{sen}\theta)$. También puede expresarse cualquier número complejo z mediante notación exponencial.

Para números reales a, b el símbolo a^b puede definirse como un número real único (Ejercicio 13, Cap. I - 12) si $a = 0$ y $b > 0$; si $a > 0$ y b es cualquier número real; y cuando $a < 0$ y $b = r/s$ donde los enteros r, s no tienen factores comunes y s es impar. El valor único del símbolo a^b se basa en el hecho de que para los valores racionales de $b = r/s$, en que r, s son enteros sin factores comunes, la ecuación $x^s = a^r$ tiene una solución positiva única en el conjunto de los números reales cuando $a^r > 0$; y tiene una solución real única en todos los otros casos tales que a^b esté definido. Ya que la ecuación $x^s = a^r$ tiene s soluciones en el sistema de números complejos, el símbolo $a^{r/s}$ puede asociarse con cualquiera de los números complejos s. De aquí que, en nuestra definición de a^b en el sistema de números complejos, será necesario a veces designar un elemento particular de un subconjunto de los números complejos, como el *valor principal* de un símbolo dado a^b.

La representación exponencial $z = re^{i\theta}$, donde e es la base de los logaritmos naturales, puede deducirse de la representación trigonométrica $z = r(\cos\theta + i\operatorname{sen}\theta)$ por medio de series infinitas. Los lectores que no recuerden las siguientes series infinitas de sus estudios anteriores de matemáticas, pueden revisar el desarrollo de estas series en el Cap. III - 15 o aceptar la representación $z = re^{i\theta}$ como una suposición más.

La serie infinita

$$e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

puede usarse para definir e^x para cualquier número complejo x (Cap. III - 15). Obtenemos entonces

$$e^{ix} = 1 + ix - \frac{x^2}{2} - \frac{ix^3}{3!} + \frac{x^4}{4!} + \frac{ix^5}{5!} - \cdots$$

substituyendo ix por x. Una comparación de esta serie con las dos series siguientes

$$\cos x = 1 - \frac{x^2}{2} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots,$$

$$\text{sen } x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots$$

indica que $e^{ix} = \cos x + i \text{ sen } x$. De esta manera, tenemos tres representaciones para un número complejo, $z = a + bi = r(\cos\theta + i \text{ sen } \theta = re^{i\theta}$. Las condiciones para la igualdad de dos números complejos z_1, z_2 son $a_1 = a_2$, $b_1 = b_2$, cuando los números están expresados en la primera forma. Cuando se emplean las otras dos formas las condiciones son $r_1 = r_2$, $\theta_1 = \theta_2 + 2k\pi$ para algún entero k. En general, encontraremos más útil la primera forma cuando estudiemos sumas de números complejos, y una de las otras formas cuando tratemos los productos o potencias.

La suma de $z_1 = a + bi$ y $z_2 = c + di$ se ha definido (Cap. 1-15) como $z_1 + z_2 = a + c + (b + d)i$. Para encontrar geométricamente la suma de dos números complejos z_1, z_2 representados por P_1 y P_2, respectivamente, se construye el paralelógramo que

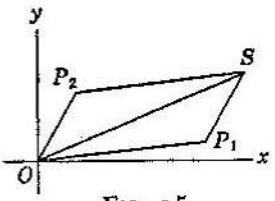


FIG. 1-5

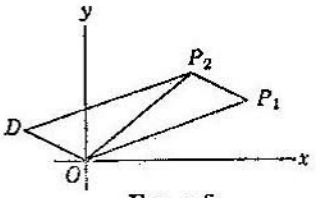


FIG. 1-6

tiene OP_1 y OP_2 como lados (Fig. 1-5). La diagonal OS del paralelogramo es el vector que representa $z_1 + z_2$. La diferencia $z_2 - z_1$ puede construirse como un lado OD de un paralelogramo con diagonal OP_2 y un lado OP_1 (Fig. 1-6).

El producto z_1z_2 se define como $z_1z_2 = ac - bd + (ad + bc)i$, pero se interpreta con más facilidad en la forma $z_1z_2 = r_1e^{i\theta_1} \cdot r_2e^{i\theta_2} = r_1r_2e^{i(\theta_1 + \theta_2)}$. La fórmula $z_1z_2 = r_1r_2[\cos(\theta_1 + \theta_2) + i \text{ sen } (\theta_1 + \theta_2)]$ puede verificarse trigonométricamente. Luego, mediante la inducción matemática como en el Teorema 1-2, se tiene (Ejercicio 8).

TEOREMA 1-4. *El valor absoluto del producto de dos o más números complejos es el producto de sus valores absolutos; el argumento del producto es la suma de sus argumentos.*

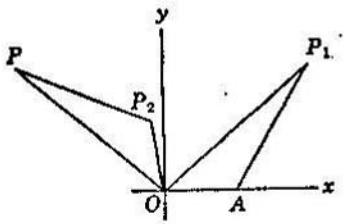


FIG. 1-7

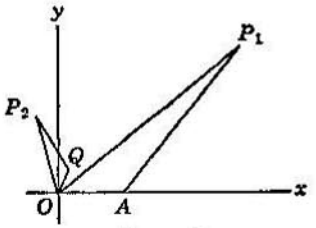


FIG. 1-8

Para encontrar geométricamente el producto z_1z_2 representado por P_1P_2, constrúyase el triángulo OP_2P semejante al triángulo OAP_1 donde $O = (0,0)$ y $A = (1,0)$ (Fig. 1-7). Entonces P es el punto que representa $z_1 \cdot z_2$. En esta construcción los dos triángulos OAP_1 y OP_2P deben estar orientados de manera análoga. Por ejemplo, si el interior del triángulo OAP_1 *está* a la izquierda al recorrer el perímetro del triángulo desde O hacia A, hacia P_1, hacia O, también el interior del triángulo OP_2P debe encontrarse a la izquierda al recorrer su perímetro en el sentido OP_2P. Los triángulos OAP_1 yOP_2P se encuentran orientados en forma análoga en la Fig. 1-7; los triángulos OAP_1 y OP_2Q están orientados inversamente en la Fig. 1-8.

La construcción geométrica correspondiente a un cuociente z_2/z_1 se obtiene construyendo los triángulos OP_2Q y OP_1A orientados en el mismo sentido (Fig. 1-8). Por medio de $z_2/z_1 = (r_2/r_1)e^{i(\theta_2-\theta_1)}$ se obtiene el teorema correspondiente al Teorema 1-4: el valor absoluto del cuociente de dos números complejos es el cuociente de sus valores absolutos; el argumento del cuociente es igual al argumento del dividendo menos el argumento del divisor.

Como en el caso de los números reales, las operaciones inversas de sustracción y división pueden evitarse calculando los números inversos $-z$ y $1/z$, respectivamente. Si $z = a + bi$, entonces $-z = -a - bi = r\,[\cos(\pi + \theta) + i \operatorname{sen}(\pi + \theta)] = re^{i(\pi+\theta)}$, de acuerdo con el Teorema 1-4 y con $-1 = \cos\pi + i \operatorname{sen}\pi$. También si $r \neq 0$, $1/z = 1/r\,[\cos(-\theta) + i \operatorname{sen}(-\theta)] = 1/r\,(\cos\theta - i \operatorname{sen}\theta)$, aplicando el enunciado correspondiente para los cuocientes y también

$$1 = 1\ (\cos 0 + i \operatorname{sen} 0).$$

Ya se ha examinado la suma, la diferencia, el producto y el cuociente de dos números complejos. Con la excepción de las relaciones de orden, todas las reglas anteriores se satisfacen en el sistema de números complejos. No hay ninguna definición satisfactoria de la magnitud o medida de un número complejo que pueda usarse para ordenar linealmente el conjunto de todos los números complejos. En efecto, hemos visto que los números complejos corresponden a los puntos de un plano en vez de a una línea recta. Por consiguiente, no cabría esperar que las relaciones de orden estudiadas anteriormente para los números reales se cumplieran para los números complejos. Los números complejos son densos y continuos, siempre que las definiciones de estos términos se formulen para conjuntos no lineales.

La importancia fundamental de los números complejos reside en el hecho de que ellos permiten calcular dos raíces para cualquiera ecuación de segundo grado $x^2 + 2ax + b = 0$, con coeficientes reales sin restricción respecto del signo de $a^2 - b$. En efecto, las n raíces de cualquier ecuación polinomia de grado n (Cap. III-1 y Teorema IV-2) con coeficientes complejos pueden expresarse como números complejos (Cap. I-18). Esta propiedad se explica diciendo que el sistema de los números complejos es *cerrado algebraicamente* (ver Bibliografía Nº 7, pág. 393). Las raíces de las ecuaciones $w^2 = z$, $w = z^2$ y, en general, $w^n = z$, $w = z^n$ para cualquier entero positivo n y para cualquier número complejo dado z han sido de particular interés para los matemáticos y se estudiarán en el Cap. I-17.

EJERCICIOS

1. Expresar cada uno de los siguientes números complejos en la forma $r(\cos\theta + i \operatorname{sen}\theta)$:

a) $1 + i$, c) 15, e) $-8 + 8i\sqrt{3}$,
b) $2 - 2i$, d) $7i$, f) -3.

2. Expresar cada uno de los números complejos del Ejercicio 1 en la forma $re^{i\theta}$.

3. Sumar gráficamente los siguientes pares de números:

(a) $3 - i$, $5 + 2i$, (c) $\sqrt{5} - \sqrt{-1}$, $2 - \sqrt{-16}$,
(b) $3 + \sqrt{-27}$, i, (d) $2 + 2\sqrt{-3}$, $\dfrac{1 + i\sqrt{2}}{2}$.

4. Multiplicar gráficamente los pares de números del Ejercicio 3 y comprobar las respuestas algebraicamente.

5. Sustraer gráficamente el primer número del segundo en cada ítem del Ejercicio 3 y comprobar las respuestas algebraicamente.

6. Dividir gráficamente el primer número por el segundo en cada ítem del Ejercicio 3 y comprobar las respuestas algebraicamente.

7. Establecer las condiciones necesarias para que sean válidas las siguientes igualdades:

$$\text{(a) } |z_1 + z_2| = |z_1| + |z_2|,$$
$$\text{(b) } |z_1 - z_2| = |z_1| - |z_2|.$$

8. Demostrar el Teorema 1-4.

1-17 TEOREMA DE DE MOIVRE. Dado cualquier número complejo $z = re^{i\theta}$ y cualquier entero positivo n, se ha establecido que z^n representa el producto de n factores z. Luego, de acuerdo con el Teorema 1-4, se tiene $z^n = r^n e^{in\theta}$. De manera análoga, para cualquier número complejo dado $z = re^{i\theta}$ y cualquier entero positivo n, las n raíces complejas de la ecuación $w^n = z$ pueden expresarse en la forma:

$$z^{1/n} = (re^{i\theta})^{1/n} = r^{1/n}e^{(\theta+2k\pi)i/n}$$

para $k = 0, 1, 2, \ldots, n - 1$, teniendo en cuenta que θ está determinado sólo para valores dentro de los límites de un múltiplo de 2π. Los valores $k = n, n+1, \ldots$, no se usan, dado que el seno y el coseno $(\theta + 2k\pi)/n$ tienen valores iguales para $k = n$ y $k = 0$, para $k = n+1$ y $k = 1$, ... Sin embargo, en ambos casos z^n y $z^{1/n}$, los resultados se obtienen y se recuerdan más fácilmente por medio de las reglas corrientes para los exponentes.

El símbolo z^n tiene un valor único para cualquier entero positivo n. El símbolo $z^{1/n}$ puede tomar cualquiera de los valores de n en el sistema de números complejos. Si z es un número real, los valores posibles del símbolo $z^{1/n}$ incluyen el valor real representado por $z^{1/n}$ en el conjunto de los números reales. Este valor se llama el valor principal (Cap. 1-16) de $z^{1/n}$ en el conjunto de los números complejos. Puede obtenerse haciendo $k = 0$ cuando z es positivo, y haciendo $k = (n - 1)/2$ cuando z es negativo y n es impar. Cuando z es negativo y n es par, el valor principal de $z^{1/n}$ se obtiene ha-

ciendo $k = 0$. No intentaremos designar valores principales para $z^{1/n}$ cuando z es imaginativo.

Consideremos, por ejemplo, $z = 2 + 2i\sqrt{3}$ con $r = 4$ y $\theta = 60^\circ = \pi/3$, es decir, $z = 4e^{\pi i/3}$. Tenemos entonces $z^2 = 16e^{2\pi i/3}$ y $z^{1/2} = 2e^{(\pi/3+2k\pi)i/2}$, donde $k = 0,1$. Usaremos, en seguida, la relación $e^{ix} = \cos x + i \operatorname{sen} x$ (Cap. 1-16) para expresar z^2 y $z^{1/2}$ en la forma $a + bi$. En particular, $z^2 = 16 (\cos 2\pi/3 + i \operatorname{sen} 2\pi/3) = 16 (\cos 120^\circ + i \operatorname{sen} 120^\circ) = -8 + 8i\sqrt{3}$. Para $k = 0$, $z^{1/2} = 2 (\cos \pi/6 + i \operatorname{sen} \pi/6) = \sqrt{3} + i$; para $k = 1$, $z^{1/2} = 2 (\cos 7\pi/6 + i \operatorname{sen} 7\pi/6) = -\sqrt{3} - i$. Si hacemos $k = 2$, entonces $z^{1/2} = 2 (\cos 13\pi/6 + i \operatorname{sen} 13\pi/6) = 2 (\cos \pi/6 + i \operatorname{sen} \pi/6)$, y obtendremos el mismo valor de $z^{1/2}$ que para $k = 0$. El teorema siguiente enuncia en forma general estos resultados.

TEOREMA 1-5. TEOREMA DE DE MOIVRE. *Si n es un entero positivo cualquiera y $z = r (\cos \theta + i \operatorname{sen} \theta)$, entonces,*

$$z^n = [r (\cos \theta + i \operatorname{sen} \theta)]^n = r^n (\cos n\theta + i \operatorname{sen} n\theta) = r^n e^{in\theta};$$

$$z^{1/n} = r^{1/n} \{\cos [(\theta + 2k\pi)/n] + i \operatorname{sen} [(\theta + 2k\pi)/n]\}$$

$$= r^{1/n} e^{i(\theta+2k\pi)/n}, \quad k = 0, 1, 2, \ldots, n - 1.$$

Este teorema se aplica a cualquier número complejo $z = re^{i\theta}$ y a enteros positivos n para expresar el número complejo único z^n y las n raíces complejas de la ecuación $w^n = z$. Cada una de estas n raíces tiene el valor absoluto $r^{1/n}$, es decir, cada una está representada por un punto en un círculo de radio $r^{1/n}$ con centro en el origen. Estos puntos están situados a iguales distancias sobre el círculo, ya que, cuando se calculan en el orden de los valores correspondientes de k, sus amplitudes difieren en múltiplos consecutivos de $2\pi/n$. En el ejemplo anterior de $z = 2 + 2i\sqrt{3}$, las dos raíces de $w^2 = z$ tenían amplitudes de $\pi/6$ y $\pi/6 + 2\pi/2 = 7\pi/6$, respectivamente, y ambas tenían el valor absoluto 2. En general se tiene,

TEOREMA 1-6. *Cualquier número complejo $z = r (\cos \theta + i \operatorname{sen} \theta)$ no igual a cero tiene exactamente n raíces complejas distintas de orden n que pueden representarse por n puntos situados a distancias iguales sobre un círculo de radio $r^{1/n}$.*

En particular, para $z = 1$, las raíces cúbicas de la unidad satisfacen,

$$w^3 = 1 = 1 \ (\cos 0 + i \operatorname{sen} 0)$$

y, por lo tanto, puede expresarse como,

$$w = 1^{1/3} \left[\cos (0 + 2k\pi)/3 + i \operatorname{sen} (0 + 2k\pi)/3\right]$$

para $k = 0, 1, 2$ o como,

$$w_1 = 1 (\cos 0 + i \operatorname{sen} 0) = 1,$$
$$w_2 = 1 (\cos 120^\circ + i \operatorname{sen} 120^\circ) = -\tfrac{1}{2} + i\sqrt{3}/2,$$
$$w_3 = 1 (\cos 240^\circ + i \operatorname{sen} 240^\circ) = -\tfrac{1}{2} - i\sqrt{3}/2.$$

Los puntos que representan w_1, w_2, w_3, son los vértices de un triángulo equilátero inscrito en un círculo de radio igual a la unidad con el origen por centro y que tiene un vértice en (1,0) sobre el eje positivo x. En general, las n-ésimas raíces de la unidad están representadas por los vértices de un polígono regular de n lados inscrito en el círculo de radio unidad, con un vértice en (1,0) sobre el eje positivo x.

Considerado desde un punto de vista ligeramente diferente, las n-ésimas raíces de la unidad forman un grupo (Cap. 1 - 14) de n elementos. Se llama un *grupo cíclico,* ya que todo elemento del grupo puede expresarse en función de un solo elemento. En el ejemplo anterior, $w^3 = 1$, las tres raíces pudieron expresarse como w_1, w_1^2, w^3_1, o como w_3, w^2_3, w^3_3. Una raíz n-ésima de la unidad, es una *raíz n-ésima primitiva* de la unidad si n es el entero positivo menor m tal que $s^m = 1$, es decir, según la terminología de la teoría de grupos, las raíces n-ésimas primitivas son aquéllas de *orden n*.

Según el Teorema de De Moivre, las raíces n-ésimas de la unidad que se obtienen de $x^n = \cos 0 + i \operatorname{sen} 0 = 1$ son $\cos 2k\pi/n + i \operatorname{sen} 2k\pi/n$ siendo $k = 0, 1, 2, \ldots, n - 1$. En particular, para $k = 1$ la raíz $w = \cos 2\pi/n + i \operatorname{sen} 2\pi/n$ es una raíz n-ésima primitiva, dado que $w^t = \cos 2t\pi/n + i \operatorname{sen} 2t\pi/n$ puede igualarse a la unidad si y sólo si t es un múltiplo de n, es decir, si n es la potencia positiva menor de w que es igual a la unidad. Por consiguiente, existe por lo menos una raíz n-ésima primitiva de la unidad para cualquier entero positivo n. Procederemos ahora a encontrar todas las raíces n-ésimas (no necesariamente primitivas) a partir de una sola raíz n-ésima primitiva de la unidad.

Dada cualquiera raíz n-ésima primitiva de la unidad s y cualquier entero t, se tiene $(s^t)^n = (s^n)^t = 1^t = 1$, de donde cualquier potencia entera positiva de una raíz n-ésima primitiva es también

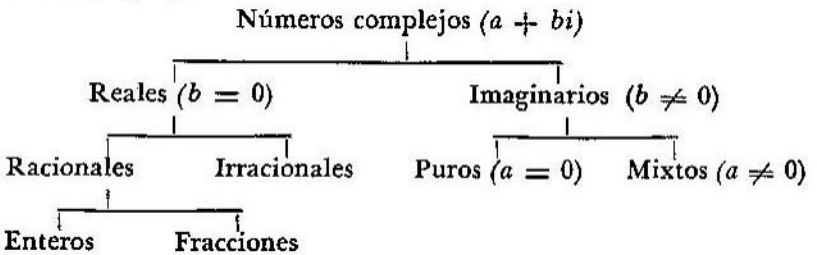
una raíz n-ésima de la unidad. También, si $s^t = s^u$, podemos suponer que $u \leqq t$ y escribir $s^{t-u} = 1$. Pero n es la potencia menor de s que es igual a la unidad, puesto que s es una raíz n-ésima primitiva. De aquí que, o bien $t = u$ o $t - u$ es un múltiplo de n (Cap. II - 2 y Teorema II - 8), es decir, $s^t = s^u$ si y sólo si $t = u + kn$ para algún entero k. En consecuencia, hemos demostrado que los números $s, s^2, s^3, \ldots, s^n = 1$ son raíces n-ésimas distintas de la unidad. Conforme a la suposición (Teorema IV - 2) de que la ecuación polinomia $z^n - 1 = 0$ tiene n raíces, se tiene el

TEOREMA I-7. *Si es es una raíz n-ésima primitiva de la unidad, todas las raíces n-ésimas de la unidad están dadas por la sucesión*

$$s, s^2, s^3, \ldots, s^{n-1}, s^n = 1.$$

Más adelante encontraremos (Teorema II - 17) que las raíces n-ésimas primitivas de la unidad son precisamente los números s^t en donde t y n son primos entre sí y s es cualquiera raíz n-ésima primitiva de la unidad.

El estudio de los grupos es de considerable importancia en las teorías matemáticas. Los examinaremos más adelante a medida que estudiemos unos cuantos conceptos abstractos más en el Cap. I - 18. Hasta aquí hemos considerado las propiedades de los enteros positivos (Cap. I-4) y a partir de éstos hemos desarrollado los sistemas de los números racionales, reales y complejos y hemos examinado las aplicaciones y las ventajas de cada sistema. Aceptando algunas igualdades tales como $a + 0 \cdot i = a$ y $a/1 = a$, podemos considerar que el sistema de números complejos es "nuestro sistema de números" y que los otros conjuntos de números son subconjuntos de él. El cuadro siguiente señala algunas de estas subdivisiones del sistema de números complejos y las condiciones que se establecen en cada caso para los números reales a, b, en la expresión $a + bi$ del número complejo general.



Los números reales pueden también clasificarse en positivos, cero o negativos; y los números complejos en algebraicos o trascendentes.

El sistema de números complejos puede considerarse de este modo como la base de nuestro estudio sobre los conceptos fundamentales del álgebra. El próximo capítulo, la teoría elemental de los números, se ocupa de algunas propiedades especiales de los números enteros. En particular, se considerarán propiedades suficientes para demostrar que todos los decimales periódicos representan números racionales y a la inversa (Cap. II - 7). Los polinomios tienen muchas propiedades análogas a aquéllas de los enteros y en el Capítulo III se hace un estudio paralelo de la teoría de los polinomios antes de tratar la teoría de las ecuaciones polinomias en el Capítulo IV.

EJERCICIOS

1. Sin emplear el Teorema de De Moivre, encontrar las raíces cuadradas de $11 - 60i$, $5 + 12i$, $-i$, $24 + 70i$, $-4ab + (2b^2 - 2a^2)i$.

(Indicación: suponer que $\sqrt{z} = x + iy$, y determinar x e y).

2. Encontrar z mediante el Teorema de De Moivre en los siguientes casos: $z^4 = 16$; $z^3 = -27$; $z^4 = i$; $z^3 = 8i$, $2^3 = 4 + 4\sqrt{-3}$.

3. Desarrollar $(\cos\theta + i \operatorname{sen}\theta)^3$ mediante el Teorema de De Moivre. Desarrollarlo también por medio del teorema del binomio y obtener de este modo fórmulas para $\cos 3\theta$ y $\operatorname{sen} 3\theta$.

4. Demostrar que los números 1, -1, i, $-i$ forman un grupo (Cap. I-14) respecto de la multiplicación.

5. Encontrar las cinco raíces de la unidad y representarlas gráficamente.

6. Encontrar todos los valores de $\sqrt[5]{1 + i}$ y de $\sqrt[3]{i}$ y representarlos gráficamente.

7. Desarrollar valiéndose del Teorema de De Moivre:

$(2\sqrt{3} - 2i)^5$; $[4\ (\cos 150° + i \operatorname{sen} 150°)]^4$

8. Encontrar las tres raíces cúbicas de -27, $-i$, $1 + i$.

9. Si w, w' son las raíces cúbicas complejas conjugadas de la unidad, demostrar que

$1 + w + w^2 = 0$, $w' = w^2$, $w = w'^2$, $w \cdot w' = 1$.

10. Indicar las raíces de la ecuación $z^n - 1 = 0$.

11. Hacer un cuadro señalando cuáles de los catorce conjuntos de números (complejos, imaginarios, imaginarios puros, imaginarios mixtos, reales, racionales, irracionales, enteros, fraccionarios, positivos, cero, negativos, algebraicos, trascen-

dentes) mencionados anteriormente son cerrados (Cap. 1-2) respecto a (a) la adición; (b) a la sustracción; (c) la multiplicación; (d) la división.

12. Hacer un cuadro como en el Ejercicio 11, señalando cuáles de los catorce conjuntos de números son (a) grupos respecto a la adición; (b) grupos respecto a la multiplicación, después de excluir el cero de aquellos conjuntos que contienen el cero; (c) campos (es decir, sistemas de números conmutativos).

13. Demostrar que las raíces n-ésimas de la unidad forman un grupo cíclico para cualquier entero positivo n.

1-18* CAMPOS Y SISTEMAS DE NUMEROS. La analogía a que nos referimos anteriormente entre las propiedades de los polinomios y las de los números enteros se debe a que ambos conjuntos forman anillos (se definirán en breve). En la presente sección estudiaremos unos cuantos conceptos fundamentales pero algo abstractos relacionados con nuestro sistema de números. Los conceptos de grupo, campo y sistema de números se han definido en el Cap. 1 - 14. En esa sección (Cap. 1 - 14) se mostró también que el conjunto de los números racionales forma el campo menor (sistema de números conmutativos) que contiene a los enteros positivos. En la presente sección consideraremos un estudio de los números complejos por adjunción (se definirá luego) de números a los conjuntos de los números racionales y reales. Observaremos también que el conjunto de los números complejos forma un campo en el cual toda ecuación polinomia de una incógnita con coeficientes pertenecientes al sistema de números complejos puede factorizarse en factores lineales.

Empezaremos con los enteros positivos o números naturales. Con el objeto de formar un grupo respecto de la adición debemos incluir los enteros negativos y cero. El conjunto de todos los enteros forma un anillo. En general, un conjunto de elementos para los cuales la adición y la multiplicación están definidas unívocamente, forma un *anillo* si los elementos del conjunto

(i) forman un grupo conmutativo respecto de la adición;
(ii) son cerrados con respecto a la multiplicación;
(iii) satisfacen la ley asociativa de la multiplicación, y
(iv) satisfacen la ley distributiva de la multiplicación con respecto a la adición (Cap. 1 - 14).

El conjunto de los números enteros pares satisface la definición anterior y forma un anillo. Por consiguiente, existen anillos de

números que no contienen a la unidad, el elemento de identidad para la multiplicación.

Un *campo* puede definirse como un anillo en el cual

(i) hay un elemento de identidad, la unidad, con respecto a la multiplicación;

(ii) la multiplicación es conmutativa, y

(iii) todos sus elementos, con excepción de cero, tienen un inverso respecto de la multiplicación.

Por consiguiente, cualquier conjunto de elementos (por ejemplo, el conjunto de los números racionales, reales o complejos) que forma un campo, forma también un anillo, pero no a la inversa. Los números enteros forman un anillo, pero no forman un campo. En general, los elementos de un anillo o de un campo no son necesariamente números. Por ejemplo, el conjunto de todos los polinomios en la variable x con coeficientes enteros forma un anillo; el conjunto de todas las funciones racionales en x con coeficientes enteros forma un campo. Un amplio tratado de grupos, anillos, y campos se puede consultar en las Bibliografías N.os 7 y 52 y un estudio muy ameno en el Nº 34 de la misma.

En el Cap. 1-8 ampliamos el conjunto de los enteros positivos considerando cuocientes a/b donde a y b eran enteros positivos. En general, podemos asociar con cualquier anillo los cuocientes a/b donde a y $b \neq 0$ sean elementos de un anillo y b no sea un divisor cero (Cap. 1-14). Este conjunto de cuocientes forma un campo y se denomina el *campo cuociente* del anillo. Por consiguiente, el campo cuociente del anillo de los enteros es el campo de los números racionales, R.

El campo R puede ampliarse por *adjunción* (tal como se describe en la frase que sigue) de un elemento k que no pertenezca a R. El campo ampliado se compone de todos los cuocientes (denominador diferente de cero) de los polinomios en k con coeficientes pertenecientes a R. Si k es un elemento de R no se obtiene nada nuevo. El conjunto de todos los polinomios en k con coeficientes pertenecientes a R forma un anillo que se designa por $R[k]$. El conjunto de todas las funciones racionales de k (cuocientes de polinomios en que el polinomio del denominador es diferente de 0) con coeficientes pertenecientes a R forma un campo que se designa por $R(k)$.

El campo $R(k)$ se llama una *ampliación algebraica* del campo R si k es una raíz de un polinomio $f(x)$, no idéntico a cero, con coeficientes pertenecientes a R.

Por ejemplo, el anillo $R[\sqrt{2}]$ comprende a todos los números de la forma $a + b\sqrt{2}$, donde a y b pertenecen a R; el campo $R(\sqrt{2})$ también comprende a todos los números $a + b\sqrt{2}$, ya que

$$\frac{c + d\sqrt{2}}{e + h\sqrt{2}} = \frac{c + d\sqrt{2}}{e + h\sqrt{2}} \cdot \frac{e - h\sqrt{2}}{e - h\sqrt{2}} = a + b\sqrt{2}$$

para un valor adecuado de a y b en R. En general, el anillo $T[k]$, que se obtiene por adjunción de un número k que es algebraico con respecto a T, en un campo T, es también un campo, es decir, $T[k] = T(k)$ cuando k es algebraico con respecto a T. Empleando una terminología que no se ha definido en este capítulo pero que es familiar a casi todo el mundo, podemos demostrar el enunciado anterior de la manera siguiente: supongamos que $f(k) = 0$ y consideremos $g(k)/h(k)$ en donde $f(x)$, $g(x)$ y $h(x)$ son polinomios, $f(x)$ es irreducible con respecto a T, y $h(k) \neq 0$. Luego, $f(x)$ y $h(x)$ tienen como máximo factor común a la unidad, de donde, según el Algoritmo de Euclides (Cap. III - 7) resultan polinomios $p(x)$ y $q(x)$ tales que

$$p(x)f(x) + q(x)h(x) = 1.$$

Dado que $f(k) = 0$, tenemos $q(k)h(k) = 1$, de donde

$$\frac{g(k)}{h(k)} = g(k) \cdot q(k)$$

es un polinomio en k, es decir, $T[k] = T(k)$.

Finalmente, dado el anillo de los enteros con campo cuociente R, buscamos un campo T tal que todo polinomio $f(x)$ con coeficientes pertenecientes a R, se factorice completamente en factores lineales (cada uno con coeficientes pertenecientes a T). Dado que $f(x)$ puede ser lineal, todo elemento de R es un elemento de T. Por consiguiente, T es un campo ampliado de R. Supongamos que tratáramos de construir T por adjunción de números a R. Con el objeto de factorizar $x^2 - 2$ se debe adjuntar $\sqrt{2}$ y se obtiene $R(\sqrt{2})$. Análogamente, para cualquier número primo 2, 3, 5, 7, 11, 13, 17, ... se debe adjuntar $\sqrt{p}$ con el objeto de factorizar

$x^2 - p$ en factores lineales. En el Cap. II - 3 se demostrará que existen infinitos números primos. Por consiguiente, no bastará ningún número finito de adjunciones a R de la forma $\sqrt{p}$, ni aún para factorizar todas las expresiones cuadráticas de la forma $x^2 - p$, y por lo tanto, es necesario enfocar el problema de algún otro modo.

Una manera de abordar este problema implica el concepto de continuidad (Cap. I - 12), y por lo tanto se necesita para esto el campo R^* de los números reales. El campo R^* contine $\sqrt{p}$ de todos los números primos p y por consiguiente es suficiente para factorizar polinomios de la forma $x^2 - p$. Ya que los números reales son infinitos no se puede esperar obtener R^* por medio de un número finito de ampliaciones algebraicas de R.

El campo de los números complejos R^* (i) constituye una ampliación algebraica de R^*, dado que i satisface la ecuación $x^2 + 1 = 0$. Se puede demostrar también que el campo R^* *(i)* no puede ampliarse más, algebraicamente, es decir, que todo polinomio de grado positivo con coeficientes pertenecientes a R^* *(i)* tiene todas sus raíces en R^* *(i)*. Este resultado se demuestra frecuentemente en dos etapas. Primero se demuestra el Teorema Fundamental del Algebra (Teorema IV - 3): Todo polinomio $p(x)$ de grado positivo con coeficientes complejos tiene por lo menos un cero complejo. En seguida se demuestra el Teorema IV - 2: Todo polinomio de grado $m > 0$ con coeficientes complejos tiene precisamente m ceros complejos (no necesariamente distintos). Existen varias demostraciones del Teorema Fundamental del Algebra, y todas implican conceptos no algebraicos (ver Bibliografía Nº 7; pág. 114). Por este motivo, se remite al lector a la (Bibliografía Nº 7; págs. 113-115) y a otros textos análogos en busca de una prueba intuitiva. En el Capítulo IV adoptaremos el Teorema IV - 3 sin demostración y lo aplicaremos en la demostración del Teorema IV - 2. Se puede demostrar también (Bibliografía Nº 7; pág. 393) que todo polinomio con coeficientes algebraicos tiene todas sus raíces en el conjunto de los números algebraicos (Cap. I - 10). En otras palabras, cualquier polinomio con coeficientes algebraicos puede factorizarse en factores lineales con coeficientes algebraicos. En la mayoría de los textos de álgebra abstracta puede consultarse una explicación más amplia de los temas tratados en esta sección.

EJERCICIOS

1. Demostrar que el conjunto de los números de la forma $3n$, donde n es un entero, forma un anillo.

2. ¿Forman los decimales exactos (Cap. I-10) un grupo respecto de la adición? ¿Un anillo?

3. Determinar cuáles de los conjuntos de números del Ejercicio 1, Cap. I-14, forman anillos.

4. ¿Cuáles de los catorce conjuntos de números del Ejercicio 11, Cap. I-17, forman anillos?

5. Demostrar que $R[\sqrt{3}] = R(\sqrt{3})$.

6. Demostrar en forma intuitiva y por escrito que los números complejos son cerrados algebraicamente.

7. Demostrar que $R[\sqrt[3]{2}] = R(\sqrt[3]{2})$.

8. Demostrar que $R[\sqrt[4]{2}] = R(\sqrt[4]{2})$.

CAPITULO II

Teoría de los números

Las propiedades de los enteros —positivos, negativos y cero— pueden aprovecharse para resolver varios tipos de problemas. Ellas son también de una importancia considerable en las teorías matemáticas. Por esta razón continuaremos nuestro estudio del sistema de números y examinaremos algunas de las propiedades especiales del conjunto de los números enteros. Según las definiciones y postulados enunciados en el Capítulo 1, los enteros

(i) forman un grupo conmutativo con respecto a la adición (Cap. 1 - 14);

(ii) son cerrados con respecto a la multiplicación (Cap. 1 - 5);

(iii) satisfacen la ley asociativa de la multiplicación (Cap. 1 - 5), y

(iv) satisfacen la ley distributiva de la multiplicación con respecto a la adición (Cap. 1 - 5).

Estas cuatro propiedades son precisamente las condiciones necesarias para que un conjunto de elementos forme un anillo (Cap. 1 - 18). En consecuencia, nos referiremos al conjunto de los números enteros con el nombre de *anillo de los enteros.*

El anillo de los números enteros tiene también otras tres propiedades (Cap. 1 - 5 y Cap. 1 - 14) que no son necesarias para todos los anillos:

(i) la multiplicación es conmutativa;
(ii) hay un elemento de identidad respecto de la multiplicación, que es la unidad en el anillo, y
(iii) no hay en el anillo divisores cero.

Técnicamente, estas últimas propiedades determinan que el anillo de los números enteros constituya también un *dominio de integridad.*

En este capítulo nos preocuparemos principalmente de las propiedades del anillo de los enteros. Muchas de estas propiedades son también propiedades de anillos más generales y se estudiarán como propiedades del anillo de los polinomios en el Capítulo III.

II·1 DIVISIBILIDAD. En un campo tal como el sistema de los números racionales o el sistema de los números reales, todo elemento del campo distinto de cero es divisor de cualquier otro elemento. En un anillo, tal como el anillo de los números enteros, no se puede suponer la divisibilidad de un elemento a por un elemento $b \neq 0$. Por definición, un entero b es divisor *o factor* de un entero a (se escribe $b|a$) si y sólo si $a = bc$, en donde c es un entero. Por ejemplo, $2|6$, $3|12$ y 3 es divisor de 15, pero 3 no es divisor de 8. El hecho de que si $c = 0$ todo entero $b \neq 0$ es divisor de cero, no debe confundirse con el concepto de "divisor cero" (Cap. I - 14) que se usa sólo cuando b y c son diferentes de cero. Aplicando la definición anterior, tenemos el teorema siguiente respecto de los enteros a, b, c.

TEOREMA II - 1. *Si c es divisor de b y b es divisor de a, entonces c es divisor de a. Si c es divisor de a y c es divisor de b, entonces c es divisor de $a + b$ y también de $a - b$.*

Un ejemplo de la primera parte del teorema sería $4|12$, $12|36$, y por lo tanto $4|36$. Asimismo, un ejemplo para la segunda parte del teorema sería $4|12$ y $4|32$ y por lo tanto $4|44$ en que $44 = 32 + 12$, y también $4|20$ en que $20 = 32 - 12$. Estas propiedades pueden demostrarse para enteros arbitrarios a, b, c que satisfagan las condiciones del teorema.

En la primera parte del teorema se da la condición de que c sea divisor de b y de que b sea divisor de a; es decir, existen enteros r y s tales que $b = cr$ y $a = bs$. Luego, puesto que la multiplicación es asociativa, $a = (cr)s = c(rs)$, de donde c es factor de a. Según la última parte del teorema existen enteros p y q tales que $a = cp$ y $b = cq$ de donde, según la ley distributiva de la multiplicación con respecto a la adición, $a + b = c(p + q)$ y $a - b = c(p - q)$. Esto completa la demostración del teorema.

Un número e se llama *unidad* si e es divisor de todos los elementos del conjunto. Las unidades en el anillo de los números enteros son $+1$ y -1. Sin embargo, solamente $+1$ es la unidad, o sea, el elemento de identidad respecto de la multiplicación.

El número entero 2 es un divisor común de 12 y 30. Los enteros -2, 3, -3, 6 y -6 son también divisores comunes de 12 y 30. Sin embargo, 6 es el único divisor común positivo de 12 y 30 que es divisible por todos los otros divisores comunes. Por eso se llama a 6 el máximo común divisor de 12 y 30. En general, enunciaremos las siguientes definiciones: Si c es divisor de a y c es divisor de b, entonces c es un *divisor común* de a y de b. Si c es un divisor común positivo de a y b, y todo otro divisor común d de a y b es divisor de c, entonces c es el *máximo común divisor* (MCD) de a y b, y se escribe $c = (a, b)$. Un entero cualquiera ec en donde $c = (a, b)$ y e es una unidad suele llamarse un MCD de a y b. Hemos modificado la definición corriente y determinado explícitamente al MCD positivo como *el* MCD de modo que el MCD esté unívocamente definido y coincida con el significado que se acepta para el símbolo (a, b). Luego, para cualquier conjunto finito de enteros $a_1, a_2, \ldots, a_n$, que no sean todos cero, podemos definir un máximo común divisor positivo único $c = (a_1, a_2, \ldots, a_n)$ que tenga la propiedad que todos los divisores comunes del conjunto, sean divisores de c. Tómese nota que c es divisor de c puesto que $c = c \cdot 1$.

Si $c = ka$ y $c = mb$, entonces c es un *múltiplo común* de a y b. Si c es un múltiplo común positivo de a y b y todo otro común múltiplo d de a y b es múltiplo de c, entonces c *es el minimum común múltiplo* de a y b, y se escribe $c = [a, b]$. Del mismo modo, para cualquier conjunto finito de enteros $a_1, a_2, \ldots, a_n$ que no sean todos cero, se puede determinar un mínimum común múltiplo positivo único $c = [a_1, a_2, \ldots, a_n]$ que tenga la propiedad de que todos los múltiplos comunes del conjunto sean múltiplos de c.

Se dice que dos enteros a y b son *primos entre sí* si todos sus divisores comunes son iguales a la unidad, es decir, $(a, b) = 1$. Por ejemplo, $(3, 4) = 1$; $(6,17) = 1$; $(64, 81) = 1$.

Consignamos las definiciones anteriores de términos tan familiares con el objeto de mantener nuestro pensamiento riguroso y también para que sirvan de base para consideraciones posteriores. En la sección que sigue de este capítulo examinaremos una pro-

piedad, menos familiar pero muy fundamental de los números enteros.

EJERCICIOS

1. Demostrar que si $a|b$, entonces $a|bc$ en donde c es un entero cualquiera.
2. Demostrar que si $a|b$, $a|c$, y $a|d$, entonces $a|(bx + cy - dz)$, en que x, y, z son enteros cualesquiera.
3. Demostrar que si $0 < a < b$, entonces b no es divisor de a.
4. Encontrar todos los enteros positivos N tales que todo entero positivo $n \leqq \sqrt{N}$ sea divisor de N.
5. Demostrar (a) que el conjunto de los números enteros pares forma un anillo y (b) que el conjunto de los enteros impares no forma un anillo. ¿Forma también, el conjunto de los enteros pares, un dominio de integridad?
6. Un número "perfecto" suele definirse como aquél que es igual a la suma de sus divisores positivos (excluidos el mismo número). Encontrar los primeros dos de estos números.
7. Demostrar que la suma de los cuadrados de dos enteros impares no puede ser el cuadrado de un entero.
8. Hacer los Ejercicios 1 a 4 del Capítulo I-18.
9. Determinar cuáles de los conjuntos de números del Ejercicio 1, Cap. I-14, forman dominios de integridad.

II-2 EL ALGORITMO DE LA DIVISION. Esta propiedad básica del conjunto de los enteros positivos se enuncia comúnmente como un teorema:

Si a y b son dos enteros positivos cualesquiera, existen enteros q y r, $0 \leqq q$, $0 \leqq r < a$ tales que $b = qa + r$.

Dados dos enteros positivos 1459 y 112, podríamos efectuar una división y escribir $1459 = 13 \cdot 112 + 3$. El teorema anterior simplemente establece que este uso de la división es una consecuencia lógica de nuestras definiciones y teoremas anteriores. Por eso el Algoritmo de la División, como mucho de nuestros otros teoremas, sirve para establecer un procedimiento aritmético común basado sobre el desarrollo de nuestro sistema de números que aparece en el Capítulo I.

Hay una "demostración" muy corriente del Algoritmo de la División que establece que, o bien $b = qa$, y en este caso $r = 0$, o bien, $b \neq qa$ y existe un entero q tal que $qa < b < (q + 1)a$. Por

consiguiente, existe siempre un entero r, $0 \leqq r < a$, tal que $b = qa + r$. Tal "demostración" parece razonable porque se vale solamente de propiedades familiares de nuestro sistema de números, es decir, si b se divide por a por medio de la operación de la división, entonces o bien $b = qa$ o $b \neq qa$, y existe un entero q que deja un resto menor que a. Sin embargo, uno de los propósitos del estudio del sistema de números es comprender en forma acabada cuáles son las suposiciones o postulados básicos necesarios. Otro propósito es identificar una "demostración" que señale que el resultado deseado puede obtenerse basándose sobre las suposiciones y definiciones fundamentales y en teoremas demostrados previamente. En la "demostración" anterior se han descuidado dos puntos. Primero, dados dos enteros positivos a y b, ¿existe siempre un entero N tal que $Na > b$? Segundo, si existiera por lo menos un entero N que satisfaga esta relación, ¿existe un entero menor que tal entero, es decir, un entero R tal que $(R - 1)\, a \leqq b < Ra$? La primera pregunta puede formularse así: ¿satisfacen los números enteros positivos el Postulado de Arquímedes? Y la segunda: ¿son los números enteros positivos bien ordenados?

El *Postulado de Arquímedes* establece que:

Dados dos enteros positivos cualesquiera a y b, existe un entero N tal que $Na > b$.

Esta propiedad de los enteros puede explicarse como sigue, de acuerdo con nuestras definiciones anteriores: puesto que a es un entero positivo debe ser $a = 1$ o bien $a > 1$. Si $a = 1$, entonces $ab = b$; si $a > 1$, entonces según el Capítulo I - 6, $(a - 1) > 0$, $(a - 1)\, b > 0$, $ab - b > 0$ y $ab > b$. En los dos casos, $ab + a = a(b + 1) > b$ y existe un entero $N = b + 1$ tal que $Na > b$. Por consiguiente, no necesitamos aceptar el Postulado de Arquímedes como un postulado, ya que puede demostrarse como teorema basándose sobre definiciones anteriores.

Finalmente, se dice que un conjunto de elementos está *bien ordenado* (Ejercicio 6, Cap. I - 6) si todo subconjunto no vacío de él tiene un primer elemento. Los enteros positivos son bien ordenados con respecto a la magnitud, los enteros negativos no lo son, los números racionales positivos tampoco, como tampoco es ordenado el conjunto de los números racionales de la forma de $1/n$.

La demostración de que los enteros positivos son bien ordenados es la siguiente: Sea I un subconjunto arbitrario de los enteros positivos. Se presentan tres casos según que I contenga sólo un número finito de elementos, que contenga infinitos elementos pero sólo a un número finito de elementos distintos, o que contenga infinitos elementos distintos. Si I contiene sólo un número finito de elementos, entonces existe un elemento mínimo de I, puesto que los enteros positivos están ordenados linealmente y es posible comparar los diversos elementos de un conjunto finito. Si I contiene infinitos elementos pero sólo un número finito de elementos distintos, sea N un extremo superior de los números finitos de elementos distintos de I. Entonces todo elemento de I coincide con uno de los números 1, 2, 3, . . ., N. Sea F el subconjunto de 1, 2, 3, . . ., N elementos que coincida con los elementos distintos de I. Entonces F es un conjunto finito y tiene un primer elemento que es también primer elemento de I. Por ejemplo, sea I el conjunto 1, 3, 5, 7, 1, 3, 7, 1, 3, 7, . . y $N = 10$. Todo elemento de I coincide con uno de los números 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. El conjunto F es 1, 3, 5, 7, y 1 es el primer elemento de F y de I. Si I contiene infinitos elementos distintos, sea N un elemento de I. Entonces divídase al conjunto I en dos subconjuntos I_1 e I_2, en los cuales aquellos elementos de I que sean menores que o iguales a N pertenezcan a I_1 y de modo que todos los demás elementos pertenezcan a I_2. El conjunto I_1 está limitado y tiene un elemento mínimo, llamémoslo R. Puesto que R es menor que o igual a N, también es menor que todos los elementos de I_2 y es un elemento mínimo de I.

Ahora ya hemos examinado en detalle las suposiciones que sustenta la breve "demostración" del Algoritmo de la División. Hemos descubierto que las propiedades que se suponían para los números enteros pudieron demostrarse directamente basándose sobre las suposiciones y definiciones formuladas en el Capítulo 1.

El Algoritmo de la División nos será muy útil. Desde un punto de vista práctico sirve de fundamento para la representación en base 10 de todos los números de nuestra notación decimal o indoarábica (Cap. II - 7). También se presta para un procedimiento, el Algoritmo de Euclides, empleado para encontrar el mayor divisor común de dos enteros cualesquiera (Cap. II - 5) o de dos polinomios cualesquiera en una variable (Cap. III - 7).

Consideraremos en seguida los números primos y estableceremos

las bases para un estudio acabado de los divisores o factores de cualquier entero dado que servirá como preparación para el Teorema de la Factorización Unica (Teorema II - 8).

EJERCICIOS

1. Demostrar que q y r son únicos en la relación $b = qa + r$ del Algoritmo de la División.

(Indicación: supóngase que $b = q_1a + r_1 = q_2a + r_2$ en donde $q_1 \geqq q_2$ y demuéstrese que $-a < r_2 - r_1 < a$).

2. Formule y demuestre el Postulado de Arquímedes respecto de dos números racionales cualesquiera.

3. ¿Qué propiedades debe tener un conjunto de elementos tales como 1, a, x, 5, r, 2, -1, . . . antes de que se intente demostrar que sus elementos satisfacen el Postulado de Arquímedes?

4. Señalar cuáles de los conjuntos de elementos siguientes están bien ordenados cuando se los ordena respecto a la magnitud: (a) los enteros mayores de 500, (b) los enteros mayores de -100, (c) enteros negativos, (d) números de la forma nk en que k es un número positivo dado y n es cualquier entero positivo, (e) los números racionales positivos, (f) los números irracionales positivos, (g) los números algebraicos.

5. Demostrar que los elementos de cualquier conjunto de elementos finito o numerable infinito puede ordenarse de modo que el conjunto sea bien ordenado.

6. Aprovechar el resultado del Ejercicio 5 y describir una ordenación de los números racionales de modo que el conjunto esté bien ordenado.

7. Demostrar que todo conjunto bien ordenado está ordenado linealmente (Cap. I-6).

II-3 NUMEROS PRIMOS. La clasificación que sigue de los enteros de acuerdo con los múltiplos que ellos tienen o de acuerdo con los números por los cuales son divisibles, facilitará grandemente nuestro estudio. Ya se ha definido a cero como el elemento de identidad con respecto a la adición (Cap. I - 5). Los enteros $+1$ y -1 se llaman unidades (Cap. II - 1). Se dice que un entero p que no es cero ni una unidad es *primo* si sus únicos divisores son $+p$ y las unidades. Un entero se llama *compuesto* si tiene dos o más divisores primos (no necesariamente distintos). Por ejemplo $6 = 2 \cdot 3$ y $121 = 11^2$ son números compuestos. Todos los numeros enteros pertenecen a una de estas cuatro clases: cero, unidades, primos y números compuestos. Puesto que cero no es positivo ni negativo, esto significa que todo entero positivo perte-

nece a una de las tres clases restantes y que cada entero positivo mayor que uno es primo o compuesto. En el estudio siguiente se supone que los números primos negativos se expresan en la forma ep, en que e es la unidad -1 y p es un número primo positivo. De esta manera basta con considerar únicamente a los números primos positivos.

Usaremos estas definiciones en las demostraciones de varios teoremas.

TEOREMA II - 2. *Todo entero mayor que la unidad tiene un divisor primo positivo.*

Sea m cualquier entero dado mayor que la unidad. Entonces m es primo si y sólo si sus únicos divisores positivos son m y 1. Si m no es un número primo, tiene un divisor positivo m_1, en donde $m_1 \neq m$ y $m_1 \neq 1$. Por eso, si m no es primo, puede escribirse como el producto de dos enteros positivos, $m = m_1 m_2$, en que ni m_1 ni m_2 son iguales a la unidad. Si ni m_1 ni m_2 son primos, entonces $m = m_{11}m_{12}m_{21}m_{22}$ en que ningún m_{ij} es igual a la unidad. Si ningún m_{ij} es primo, entonces $m = m_{111}m_{112}m_{121}m_{122}m_{211}m_{212}m_{221}m_{222}$, en donde ningún m_{ijk} es la unidad. Este proceso termina si y sólo si en alguna etapa, por lo menos, uno de los m es un número primo. Demostraremos en seguida que, para cualquier entero positivo dado m el proceso debe terminar y no puede continuar indefinidamente. Primero, se observará que cualquier entero positivo m_2 que no sea la unidad satisface la relación de orden $m_2 > 1$ (Cap. 1-6). Entonces se tiene también $m = m_1 m_2 > m_1$ y, en general,

$$m > m_1 > m_{11} > m_{111} > \cdots$$

para tantas etapas como las que tenga el proceso. Por consiguiente, el proceso termina si y sólo si el conjunto de enteros positivos $m, m_1, m_{11}, m_{111}, \ldots$ es un conjunto finito. En todo caso, este conjunto es un subconjunto del conjunto finito, $m, m-1, m-2, \ldots, 3, 2, 1$, y, por lo tanto, debe él mismo ser finito. De esta manera, el proceso en referencia debe terminar después de un número finito de etapas, y m debe tener un divisor primo.

También hemos demostrado que cualquier entero positivo dado m puede tener solamente un número finito de divisores enteros

positivos mayores que la unidad. El teorema siguiente indica cuáles son los enteros positivos que hay que considerar cuando se buscan los divisores positivos de un entero dado m.

TEOREMA II-3. *Si un entero positivo m es compuesto, entonces tiene un divisor primo positivo $\leqq I$, en donde I es el entero mayor cuyo cuadrado es $\leqq m$.*

Según el Teorema II-2, cualquier entero positivo m mayor que 1 tiene un divisor primo positivo p, es decir, $m = pm_1$. También si $m \neq p$, entonces m_1 tiene un divisor primo positivo $\leqq m_1$. Si el Teorema II-3 fuera falso, existiría un número m que fuera compuesto y no tuviera ningún divisor primo positivo $\leqq I$. En este caso, tendríamos $I < p$, $I < m_1$ o $I + 1 \leqq p$, $I + 1 \leqq m_1$ y $(I + 1)^2 \leqq pm_1 = m$, lo que es contrario a la suposición de que I es el entero mayor cuyo cuadrado es $\leqq m$. Por consiguiente, el Teorema II-3 debe ser verdadero (método de demostración indirecta, Cap. I-10).

Antes de que podamos aplicar el Teorema II-3 para determinar si un entero dado m, por ejemplo 359, es o no primo, necesitamos algún método para determinar los números primos $\leqq I$ en que $I^2 \leqq m < (I + 1)^2$. Para el caso de $m = 359$ necesitamos conocer los números primos $\leqq 18$.

Los números primos limitados por cualquier entero finito N pueden encontrarse por un método llamado la *Criba de Eratóstenes*, que es el siguiente: se escriben los enteros desde 1 hasta N, excluyendo el 1 puesto que es la unidad, contando a partir de 2 (se excluye el dos), tachar todos los segundos números de ahí en adelante; contando desde 3 (excluido el 3), tachar todos los terceros números de ahí en adelante, y, en general, contando desde cualquier entero k que es $\leqq \sqrt{N}$ (Teorema II-3), tachar todos los enteros de orden k. Por ejemplo, los números primos limitados por $N = 18$ son 2, 3, 5, 7, 11, 13, 17, y pudieron encontrarse del siguiente esquema:

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~,

en el cual fue sólo necesario excluir la unidad y los múltiplos de 2 y 3 ya que el entero siguiente que quedaba, 5, tiene un cuadrado mayor que 18.

Después de esto, podemos usar el Teorema II-3 y determinar si 359 es primo o no, probando sucesivamente si 359 es divisible por 2, 3, 5, 7, 11, 13, 17. Sobre esta base podemos aseverar que 359 es un número primo.

Una de las razones para considerar métodos mecánicos como el anterior para determinar números primos es que aún no se ha encontrado ninguna fórmula ni representación analítica para los números primos. Sin embargo, podremos demostrar varios teoremas referentes a los números primos. El teorema siguiente es una versión moderna de la Proposición 20 del Libro IX de los *Elementos* de Euclides.

TEOREMA II-4. *El conjunto de los números primos positivos es infinito numerable.*

Supongamos que hubiera un número primo mayor que todos los demás, por ejemplo, P, entonces $N = P! + 1$ debe tener un divisor primo (Teorema II-2). Pero ningún número $\leqq P$ es divisor de $P! + 1 = N$. Por eso, N tiene un divisor primo mayor que P y no hay ningún primo mayor que todos los demás, es decir, el conjunto de los números primos positivos es infinito numerable. Por ejemplo, si $P = 2$, entonces $N = 2! + 1 = 3$, que es primo; si $P = 5$, entonces, $N = 5! + 1 = 121$, que tiene a $11 > 5$ como divisor primo. Este procedimiento para determinar la existencia de un número primo mayor que cualquier número primo dado P, puede aprovecharse también, junto con el hecho de que existe un solo número primo 2, para demostrar por inducción matemática (Cap. I-4) que existe un subconjunto infinito numerable del conjunto de los números primos positivos. Luego, puesto que el conjunto de todos los números primos positivos es un subconjunto del conjunto de los enteros positivos, que es infinito numerable, hemos obtenido otra demostración de que el conjunto de los números primos positivos es infinito numerable.

Las propiedades más conocidas de los números primos se refieren a la divisibilidad. Dado cualquier entero m y el número primo p, los únicos divisores positivos de p, y, por lo tanto, los únicos comunes divisores positivos posibles de p y m, son p y 1. De aquí que resulte el

TEOREMA II-5. *Si p es un número primo y m es cualquier número entero, entonces p es un divisor de m o bien $(p, m) = 1$.*

Otro teorema conocido puede demostrarse como sigue: Supongamos que p es un número primo, y a y b sean cada uno enteros positivos menores que p. Deseamos demostrar que p no es divisor del producto ab, y se escribe $p \nmid ab$. Nos valdremos del método de demostración indirecta y supondremos que $p \mid ab$. Además, supondremos que b es el entero positivo menor tal que $p \mid ab$, es decir, ab es el múltiplo menor de a tal que $p \mid ab$. Esta última suposición puede hacerse sin perder la generalidad de la demostración, ya que si existe un múltiplo entero único, éste debe ser el múltiplo entero positivo menor de a que sea divisible por p (Cap. II-2). Ahora bien, según el Algoritmo de la División, existe un entero m tal que,

$$mb \leqq p < (m + 1)b, \; 0 \leqq p - mb < b.$$

En realidad, $mb \neq p$ puesto que $1 < b < p$ y p es primo. Por *suposición*, $p|ab$ y también $p|mab$. Entonces de $p|ap$ se tiene $p|(ap - mab)$ y $p|a(p - mb)$, de donde $a(p - mb)$ es un múltiplo de a que es divisible por p. Pero también $a(p - mb) < ab$, lo que es contrario a la suposición de que ab sea el menor múltiplo de a que es divisible por p. Por consiguiente, p no es divisor de ab, y hemos hecho una demostración indirecta del siguiente teorema:

TEOREMA II - 6. *Si p es un número primo, y a y b son dos enteros positivos, cada uno menor que p, entonces $p \nmid ab$.*

Este teorema puede ampliarse para dos enteros positivos cualesquiera a y b tales que $p \nmid a$ y $p \nmid b$. Sea $a = mp + r$, $b = np + s$, $0 < r < p$, $0 < s < p$. Ahora bien, si $p|ab$, tenemos también $p|rs$, lo que es contrario al Teorema II-6. Por consiguiente, si $p \nmid a$ y $p \nmid b$, entonces $p \nmid ab$. En otras palabras, si $p|ab$, entonces se verifica que $p|a$ o bien $p|b$. Puesto que el producto de dos enteros es un entero, también podemos hacer $a_1 \cdot a_2 = a$, $a_3 = b$ y demostrar que si $p|a_1a_2a_3$, entonces p es divisor de por lo menos uno de los números a_1, a_2, a_3. Por aplicación repetida de este procedimiento, tenemos

TEOREMA II-7. *Si p es un número primo y $p \mid a_1 a_2 \ldots a_n$, entonces p es divisor de por lo menos uno de los enteros $a_1, a_2, \ldots, a_n$, en donde n es un entero positivo cualquiera.*

Una aplicación muy importante de esta propiedad de los números primos se encuentra en la factorización de todos los enteros positivos como productos de potencias de números primos (Cap. II-4). En todo el resto de este libro usaremos ampliamente las propiedades de los números primos y las propiedades análogas de los polinomios irreducibles (Cap. III-6).

EJERCICIOS

1. Encontrar los números primos menores que 200, por medio de la Criba de Eratóstenes.

2. Determinar cuáles de los números siguientes son primos:

a) 85, 103, 179, 539;

b) 267, 781, 859, 937;

c) 1245, 2287.

3. Escribir una demostración rigurosa del Teorema II-7 por medio de la inducción matemática.

4. ¿Es $n^2 - n + 41$ un número primo para todos los valores enteros positivos de n? Explicar

5. Dar cuatro ejemplos numéricos para ilustrar el Teorema II-5.

6. Repetir el Ejercicio 5 para los Teoremas II-6 y II-7.

7. Dado un entero N cualquiera, ¿cómo se pueden encontrar *todos* sus divisores primos positivos?

8. Demostrar que $n^3 + 1$ es un número compuesto si n es mayor que la unidad.

9. Demostrar que $3^n - 1$ y en general, $m^n - 1$ es un número compuesto si n es mayor que uno y m es mayor que 2 (ver Ejercicio 7, Cap. I-4).

10. Un número de la forma $2^p - 1$ que sea primo se llama *número primo de Mersenne*. Encontrar cinco números de éstos.

11. Demostrar que $2^n - 1$ es un número compuesto si n es compuesto. (Ver Ejercicio 9, Cap. I-4). Dar un ejemplo de un número compuesto de la forma $2^p - 1$ en que p sea un número primo.

II-4 TEOREMA DE LA FACTORIZACION UNICA. Se dice que un entero se ha factorizado completamente cuando se ha expresado como producto de números primos (positivos) y una unidad ($+1$ o -1). En esta

sección del Cap. II tendremos en cuenta, primero, que el producto de cualquier número finito de unidades es una unidad y demostraremos que cualquier entero puede expresarse como un producto de números primos positivos y una unidad de una manera única. En seguida deduciremos algunas consecuencias más de esta factorización.

El entero positivo 168 puede expresarse como un producto de enteros de diversas maneras. Por ejemplo,

$$168 = 4 \cdot 42 = 2 \cdot (-2) \cdot (-7) \cdot 6 = 21 \cdot 8 = 7 \cdot 24.$$

El teorema de la factorización única establece que si 168 se expresa como producto de números primos positivos, $168 = 2^3 \cdot 3 \cdot 7$, cualquiera otra factorización en divisores primos tal como $168 = 3 \cdot 2^3 \cdot 7$, debe coincidir con la primera, salvo por el orden en que están escritos los divisores.

Cualquier entero positivo m mayor que 1 tiene por lo menos un divisor o factor primo positivo según el Teorema II-2. Este divisor primo, sea p_1, puede hallarse en un número finito de etapas, puesto que m es finito y p_1 es uno de los números 1, 2, 3, ..., m. Si $p_1 = m$, nuestra factorización es completa y es única. Si $p_1 \neq m$, entonces $m = p_1 m_1$ y si procedemos como anteriormente con m_1, obtendremos $m = p_1(p_2 m_2)$ si m_1 no es primo. Ya que los enteros positivos $m, m_1, m_2, \ldots$ satisfacen la relación $m > m_1 > m_2 > \ldots$, el proceso anterior, lo mismo que aquél de la demostración del Teorema II-2, debe terminar después de un número finito de pasos y resultar

$$m = p_1 p_2 \ldots p_r. \tag{II-1}$$

Si hubiera también una segunda factorización,

$$m = q_1 q_2 \ldots q_s \tag{II-2}$$

de m en divisores primos positivos, tendríamos

$$p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s. \tag{II-3}$$

Puesto que p_1 es divisor de $q_1 q_2 \ldots q_s$, debe, según el Teorema II-7, ser divisor de algún q_i, sea q_1. Ya que hemos aceptado que

q_1 y p_1 son números primos positivos, $p_1 = q_1$. Dividimos entonces ambos miembros de (II - 2) por $p_1 = q_1$ y repetimos el mismo argumento para demostrar que p_2 es igual a alguno de los números q, sea q_2. Este proceso puede continuarse hasta que uno de los miembros de (II - 3) quede reducido a 1. Puesto que los números p y q son enteros, el otro miembro debe simultáneamente hacerse igual a 1. De aquí que exista una factorización de m en divisores primos, y si se presentan dos factorizaciones (II - 1) y (II - 2) de m en divisores primos, éstas son idénticas, excepto posiblemente en el orden en que están escritos los divisores. Por consiguiente, los divisores y la factorización son únicos. Si los números primos iguales se agrupan juntos, tenemos el *Teorema de Factorización Unica* o, como suele llamarse, el *Teorema Fundamental de la Aritmética:*

TEOREMA II - 8. *Todo entero con la excepción de cero puede representarse de una y sólo una manera en la forma*

$$m = e_1 p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},$$

en que e_1 *es una de las unidades, los* p_i *son números primos positivos distintos y los* a_i *son enteros positivos.*

Por lo tanto, dado cualquier entero m, podemos elegir la unidad adecuada y entonces aplicar el Teorema II - 3 y divisiones sucesivas para encontrar los divisores primos positivos de m. Por ejemplo,

$12 = 2^2 \cdot 3$; $-36 = (-1) \cdot 2^2 \cdot 3^2$; $1232 = 2^4 \cdot 7 \cdot 11$.

Examinemos por un momento $12 = 2^2 \cdot 3$. Cualquier divisor primo de 12 debe ser divisor de 2^2 ó de 3, según el Teorema II-7. Por consiguiente, 2 y 3 son los únicos divisores primos de 12. Asimismo, todos los divisores positivos de 12 pueden expresarse en la forma $d = 2^a \cdot 3^b$, en donde $a = 0, 1, 2$ y $b = 0$ ó 1. Todos los divisores de 12 tienen la forma $e \cdot 2^a \cdot 3^b$, en donde e es una unidad, $0 \leqq a \leqq 2$, y $0 \leqq b \leqq 1$. En general, todos los divisores de $m =$ $e_1 p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ son de la forma

(II - 4) $\qquad e_1 p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, en que $0 \leqq bi \leqq a_i$

y e_k es una unidad. Además, todo número de la forma (II - 4) es un divisor de m. De este concepto de divisor y del Teorema II - 8 se desprende que

TEOREMA II-9. *Si a y b no tienen divisores comunes y cada uno de ellos es divisor de c, entonces su producto es divisor de c. Si a y c no tienen divisores comunes y b y c no tienen divisores comunes, entonces ab y c no tienen divisores comunes. Si a y c no tienen divisores comunes y c es divisor de ab entonces c es divisor de b.*

Las tres partes de este teorema se pueden expresar matemáticamente como sigue: (i) $(a,b) = 1$, $a|c$ y $b|c$ implica $ab|c$; (ii) $(a, c) = 1$ y $(b, c) = 1$ implica $(ab, c) = 1$; (iii) $(a, c) = 1$ y $c|ab$ implica $c|b$. Las demostraciones de estos enunciados se dan como ejercicios (Ejercicios 3, 4 y 5).

El Teorema II - 8 puede también usarse para encontrar el máximo común divisor y el mínimo común múltiplo de dos enteros (Cap. II - 1). Por ejemplo, si $m = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7$ y $n = 2^2 \cdot 3^3 \cdot 7^2 \cdot 11$, entonces $(m, n) = 2^2 \cdot 3^2 \cdot 7$ y $[m, n] = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11$. Estos valores particulares pueden obtenerse a la simple vista. En general, suele ser ventajoso expresar m y n por medio de los mismos números primos positivos, empleando para esto el exponente cero. Por ejemplo, en el caso anterior, $m = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11^0$ y $n = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^2 \cdot 11$. Por eso, dados dos enteros cualesquiera m y n, se puede escribir cada uno de ellos por medio de sus divisores primos positivos y en seguida expresar cada cual, como anteriormente, mediante el mismo conjunto de números primos, es decir, $m = e_j p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ y $n = e_r p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$. Estas expresiones pueden abreviarse valiéndose del símbolo para el producto $\prod$, como sigue

$$m = e_j \prod_{i=1}^{k} p_i^{a_i}, \quad n = e_r \prod_{i=1}^{k} p_i^{b_i}.$$

Entonces (m, n) se obtiene tomando el menor exponente que se presente en cada número primo p_i, y $[m, n]$ se obtiene tomando el mayor exponente que aparezca en cada número primo p_i. La nota-

ción matemática sería $(m, n) = \prod_{i=1}^{k} p_i^{c_i}$, $[m, n] = \prod_{i=1}^{k} p_i^{d_i}$, en donde c_i, es el mínimum de a_i y b_i; y d_i es el máximum de a_i y b_i.

Finalmente, supongamos $(a, b) = d$, $[a, b] = m$, y sea $a = a_1 d$, $b = b_1 d$. Entonces $(a_1, b_1) = 1$, el mínimo común múltiplo de a y b es $m = a_1 b_1 d$, y $dm = da_1 b_1 d = ab$. De este modo tenemos

TEOREMA II-10. *Si a y b son enteros positivos, $(a, b) = d$, y $[a, b] = m$, entonces $dm = ab$.*

Por ejemplo, $(6, 8) = 2$, $[6, 8] = 24$, y $6 \cdot 8 = 2 \cdot 24$. El hecho de que este teorema no pueda aplicarse directamente para el caso de tres enteros positivos se evidencia en el ejemplo siguiente: $(6, 4, 10) = 2$; $[6, 4, 10] = 60$, y $6 \cdot 4 \cdot 10 = 240 \neq 2 \cdot 60$.

En la sección que sigue de este capítulo nos serviremos del Algoritmo de Euclides para encontrar $d = (a, b)$ sin tener que expresar primeramente a y b por medio de sus divisores primos. En seguida por medio de la expresión $m = ab/d$ del Teorema II - 10 encontraremos $m = [a, b]$. Es así como luego podremos encontrar (a, b) y $[a, b]$ sin necesidad de expresar a y b en sus divisores primos.

EJERCICIOS

1. Descomponer en sus divisores primos positivos los números 4680, 1275 y 1273.
2. Encontrar (4680, 1275) y [4680, 1275] por medio de sus divisores primos. ¿Es válido el Teorema II-10 para este caso?
3. Demostrar la primera parte del Teorema II-9.
4. Demostrar la segunda parte del Teorema II-9.
5. Demostrar la tercera parte del Teorema II-9.
6. Dado cualquier entero n ¿cómo se pueden encontrar *todos* sus divisores positivos?
7. Encontrar todos los divisores positivos de 60.
8. Demostrar que todo divisor positivo de $m = e_j p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ aparece una vez y sólo una entre los términos del producto

$$(1 + p_1 + p_1^2 + \cdots + p_1^{a_1})(1 + p_2 + p_2^2 + \cdots + p_2^{a_2}) \cdots (1 + p_n + p_n^2 + \cdots + p_n^{a_n}).$$

9. Demostrar que el entero m en el Ejercicio 8 tiene $(a_1 + 1)(a_2 + 1) \cdots (a_n + 1)$ divisores positivos distintos.

10. Demostrar que la suma de los divisores positivos del entero m en el Ejercicio 8 puede expresarse en la forma

$$\prod_{i=1}^{n} \frac{p_i^{a_i+1} - 1}{p_i - 1},$$

por medio del símbolo del producto Π.

11. Determinar cuántos son y cuánto suman los divisores positivos de 60, por medio de los Ejercicios 9 y 10.

12. ¿Cuántos divisores tiene cada uno de los números del Ejercicio 1?

13. Encontrar la suma de los divisores de cada uno de los números del Ejercicio 1.

II-5 EL ALGORITMO DE EUCLIDES.

En el Cap. II - 4 se expresó el máximo común divisor (m, n) de dos enteros por medio de los divisores primos de los dos enteros. El Algoritmo de Euclides proporciona un método directo para obtener el máximo común divisor de dos enteros sin tener que expresar los enteros en sus divisores primos. Este método es ventajoso especialmente cuando se trata de números grandes. En el caso de 36 y 90, el método del Cap. II - 4 se escribiría $36 = 2^2 \cdot 3^2$ y $90 = 2 \cdot 3^2 \cdot 5$, luego $(36, 90) = 2 \cdot 3^2 = 18$. El Algoritmo de Euclides daría $90 = 2 \cdot 36 + 18$; $36 = 2 \cdot 18 + 0$; y $(36, 90) = 18$.

En general, como el máximo común divisor se considera positivo, se puede calcular para dos enteros cualesquiera diferentes de cero, tomando en cuenta sólo los enteros positivos correspondientes m, n cada vez que se presenten los factores $+1$ o -1. Si $m = n$, entonces también $(m, n) = m$; si $m \neq n$, supongamos que $m > n$. Entonces aplicamos el Algoritmo de la División repetidas veces (Cap. II - 2) y obtenemos el *Algoritmo de Euclides:*

$$\begin{aligned}
&(2\text{–}5) && m = qn + n_1, && 0 < n_1 < n \\
&(2\text{–}6) && n = q_1 n_1 + n_2, && 0 < n_2 < n_1 \\
&(2\text{–}7) && n_1 = q_2 n_2 + n_3, && 0 < n_3 < n_2 \\
& && \cdot && \cdot \\
& && \cdot && \cdot \\
& && \cdot && \cdot \\
&(2\text{–}8) && n_{k-2} = q_{k-1} n_{k-1} + n_k, && 0 < n_k < n_{k-1} \\
&(2\text{–}9) && n_{k-1} = q_k n_k. && 0 = n_{k+1}
\end{aligned}$$

Puesto que los enteros n, n_1, n_2, ... forman una sucesión decreciente, es decir, $n > n_1 > n_2 > \ldots$, existe algún entero n_k, sea n_{k+1}, igual a cero y tal que $k = 0$ o bien n_k sea diferente de cero. Encontraremos que cuando $k = 0$ $(m,n) = n = n_0$; y cuando $k \neq 0$, $(m, n) = n_k$.

Cualquier divisor común de m y n, debe ser divisor de n_1 de acuerdo con la relación (II - 5); debe ser divisor de n_2 de acuerdo con (II - 6); de n_3 de acuerdo con (II - 7), ..., y de n_k de acuerdo con (II - 8). De este modo, todo divisor común de m y n es divisor de n_k. Inversamente, n_k es divisor de n_{k-1} de acuerdo con (II - 9); de n_{k-2} de acuerdo con (II - 8), ..., de n_1 de acuerdo con (II - 7); de n de acuerdo con (II - 6); y de m de acuerdo con (II - 5), es decir, n_k es un divisor común de m y de n. Estos resultados se enuncian en el siguiente teorema:

TEOREMA II-11. *El máximo común divisor de dos enteros positivos cualesquiera m y n puede encontrarse por medio del Algoritmo de Euclides: es el último resto que no desaparece. Existen enteros A y B tales que*

$$(m, n) = n_k = Am + Bn. \tag{II - 10}$$

Los enteros A y B de (II - 10) se pueden obtener resolviendo (II - 5) para n_1 en la fórmula $n_1 = A_1m + B_1n$ y sustituyendo esto en (II - 6) para obtener $n_2 = A_2m + B_2n$, ...: finalmente $n_k = Am + Bn$ se obtiene de (II - 8). Por ejemplo, tenemos la forma siguiente del Algoritmo de Euclides para los números 23 y 19:

$$\begin{aligned} 23 &= 1 \cdot 19 + 4, \\ 19 &= 4 \cdot 4 + 3, \\ 4 &= 1 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0, \end{aligned}$$

de donde $(23, 19) = 1$. Puede encontrarse una relación de la forma (II - 10) que se indica anteriormente, por medio de las ecuaciones

$$\begin{aligned} 4 &= 1 \cdot 23 - 1 \cdot 19, \\ 3 &= 1 \cdot 19 - 4 \cdot 4 = 5 \cdot 19 - 4 \cdot 23, \\ 1 &= 1 \cdot 4 - 1 \cdot 3 = 5 \cdot 23 - 6 \cdot 19. \end{aligned}$$

Este procedimiento puede expresarse por medio de los cuocientes generales q_i y restos n_i desde (II - 5) hasta (II - 9) de la manera siguiente:

$$
\begin{aligned}
n_1 &= m - qn = A_1 m + B_1 n, \\
n_2 &= -q_1 m + (q_1 q + 1)n = A_2 m + B_2 n, \\
n_3 &= (q_1 q_2 + 1)m - (q_2 + q q_1 q_2 + q)n = A_3 m + B_3 n, \\
&\cdot \\
&\cdot \\
&\cdot
\end{aligned}
$$

Los coeficientes de m y n son enteros en todas las etapas, ya que únicamente se trata de las operaciones del anillo: la adición, la sustracción y la multiplicación.

Queda aún el problema práctico de encontrar A y B para enteros cualesquiera dados m y n con el menor trabajo posible. Para cualquier entero $m \neq 0$, tenemos $(m, 0) = em$ en donde e es una unidad. También hemos hecho notar que se puede suponer que los enteros dados son positivos sin que se pierda la generalidad de la expresión. El esquema siguiente proporciona un procedimiento práctico para determinar el máximo común divisor y una relación de la forma (II - 10) para dos enteros positivos cualesquiera m y n. Los números n_i y q_i son los mismos que los de (II - 5) hasta (II - 9). El esquema

$$
\begin{array}{cccccccc}
m & n & n_1 & n_2 & n_3 & \cdot\ \cdot & n_k & 0 \\
 & q & q_1 & q_2 & q_3 & \cdots & q_k & \\
 & 1 & -q & B_2 & B_3 & \cdots & B_k = B & \\
 & & 1 & -q_1 & A_3 & \cdots & A_k = A &
\end{array}
\tag{2-11}
$$

puede construirse por medio del diseño geométrico

$$
\begin{array}{ccc}
n_{i-1} & n_i & n_{i+1} \\
 & q_i &
\end{array}
$$

en las primeras dos filas para significar que $n_{i-1} = q_i n_i + n_{i+1}$; representando el último n_i diferente de cero por n_k, y determinando los A_i y B_i por medio de las fórmulas de recurrencia

$$B_0 = 1,\ A_0 = 0,\ B_1 = -q,\ A_1 = 1,$$
$$B_{i+1} = B_{i-1} - q_i B_i, \qquad (i = 1, 2, 3, 4, \ldots, k-1)$$
$$A_{i+1} = A_{i-1} - q_i A_i.$$

Para el caso de $m = 23$, $n = 19$, este esquema resulta ser

$$\begin{array}{cccccccc} & & 23 & 19 & 4 & 3 & 1 & 0 \\ \text{(II - 12)} & & & 1 & 4 & 1 & 3 & \\ & & & 1 & -1 & 5 & -6 & \\ & & & & 1 & -4 & 5 & \end{array}$$

de donde $(23, 19) = 1$ y $1 = 5 \cdot 23 - 6 \cdot 19$, tal como se obtuvo anteriormente.

El método anterior para obtener n_k es simplemente una representación sintética de las relaciones (II - 5) a (II - 9) y por lo tanto es válido. El método anterior para determinar A_k y B_k puede verificarse por inducción matemática respecto de j, en donde $n_j = mA_j + nB_j$. Para $j = 0$, se hace $n_0 = n$ y se tiene $n = n$; para $j = 1$ se tiene $n_1 = m - qn$, que es válido según (II - 5). Supongamos que $n_{i-1} = mA_{i-1} + nB_{i-1}$ y que $n_i = mA_i + nB_i$, entonces

$$\begin{aligned} n_{i+1} &= n_{i-1} - q_i n_i \\ &= m(A_{i-1} - q_i A_i) + n(B_{i-1} - q_i B_i) \\ &= mA_{i+1} + nB_{i+1}, \end{aligned}$$

y se verifican así las fórmulas de recurrencia dadas más arriba.

El método representado por el esquema (II - 11) puede ser muy útil después de un poco de práctica. Es ventajoso especialmente porque el máximo común divisor puede determinarse sólo por medio de las dos primeras filas. Luego, si se desea una relación de la forma (II - 10), se pueden determinar las constantes A y B.

La ecuación (II - 10) es, pues, necesaria y suficiente para que n_k sea el máximo común divisor de m y n. Es necesaria según el Teorema II - 11 y es suficiente ya que si (II - 10) es válido, todo factor común de m y n debe ser divisor de n_k. Como una aplicación particular de esto, tenemos

TEOREMA II - 12. *Dos enteros m y n son primos entre sí si y sólo si hay enteros A y B tales que $Am + Bn = 1$.*

Nos serviremos del Algoritmo de Euclides y del Teorema II - 12 para obtener el recíproco de n, módulo m en la sección 11 de este Capítulo II. En el Cap. III - 7 estos resultados se formulan nuevamente para polinomios $p(x)$. En esta forma se emplearán para encontrar el máximo común divisor de dos polinomios, el número de raíces distintas de una ecuación polinomia en cualquier intervalo $a < x \leqq b$ (Cap. IV - 12), y las raíces múltiples de una ecuación polinomia (Cap. IV - 13).

EJERCICIOS

1. ¿Cómo se puede demostrar, mediante el Algoritmo de Euclides, la existencia de un máximo común divisor entre dos enteros positivos cualesquiera?

2. Demostrar que $(km, kn) = k(m, n)$ para cualquier entero positivo k.

3. Expresar cada uno de los siguientes divisores en la forma (II-10):

a) (108, 64),
b) (370, 111),
c) (147, 64),
d) (3961, 952),
e) (4680, 1275).

Comparar con el Ejercicio 2, Cap. II-4.

4. Encontrar el mínimo común múltiplo de cada uno de los pares de números del Ejercicio 3.

5. Demostrar que $[km, kn] = k[m, n]$.

6. Demostrar que si $(a, b) = 1$, en que a y b son enteros cualesquiera, entonces existen enteros d y e tales que

$$\frac{1}{ab} = \frac{d}{a} + \frac{e}{b}.$$

7. Demostrar que todo número racional positivo puede expresarse como una fracción continua finita de la forma

$$\frac{m}{n} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_k}}}}}$$

que se suele escribir de la manera siguiente:

$$\frac{m}{n} = q + \frac{1}{q_1^+} \quad \frac{1}{q_2^+} \quad \frac{1}{q_3^+} \cdots + \frac{1}{q_k}.$$

(Indicación: Los q aquí son los mismos que en el Algoritmo de Euclides. La expresión que correspondería a (II - 12) sería

$$\frac{23}{19} = 1 + \frac{1}{4^+} \quad \frac{1}{1^+} \quad \frac{1}{3^+}.)$$

8. Aprovechese el resultado obtenido en el Ejercicio 3 y exprésese cada uno de los siguientes números racionales como fracciones continuas:

$$\frac{108}{64}, \frac{370}{111} \quad \frac{147}{64}, \frac{3961}{952}, \frac{4680}{1275}.$$

9. Demostrar que $-B/A$ en (II-10) es una aproximación de m/n que difiere de m/n en n_k/An. Esta es una primera aproximación muy práctica y es equivalente a despreciar el término q_k en el Ejercicio 7. De consiguiente $\frac{23}{19}$ es aproximadamente $\frac{6}{5}$, y en este caso el error es de $\frac{1}{114}$.

10. Emplear el método del Ejercicio 9 y encontrar las primeras aproximaciones a cada una de las fracciones del Ejercicio 8. Indicar el error de la aproximación en cada caso.

11. Continuar el procedimiento de aproximación comenzado en el Ejercicio 9 y demostrar que en general la aproximación de orden $(j + 1)$ de m/n es $-B_{k-j}/A_{k-j}$ en la fórmula (II-11).

II-6 BASES. El concepto de una "base" es tan fundamental en la teoría de los números como lo es en "baseball".

Cualquiera interpretación de un número, tal como 1776, en el cual la posición de los dígitos tiene un significado, depende del número particular que se ha elegido como base. Por ejemplo, 11 representa once en base diez, es decir, una decena y una unidad en la notación decimal. Sin embargo, 11 también representa tres en la base dos, es decir, un grupo de dos y una unidad en el sistema binario de números. Todos estamos familiarizados con la notación decimal (Cap. II - 7) que emplea la base diez y los dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. El sistema binario se sirve sólo de dos dígitos, que son 0 y 1, y ha alcanzado una importancia creciente con el desarrollo de los computadores electrónicos, puesto que sus dígitos pueden representarse por la presencia y ausencia, respectivamente, de una corriente eléctrica. En general, demostraremos que todo entero positivo n mayor que 1 puede usarse como base para todos los enteros positivos, es decir,

TEOREMA II - 13. *Si m y n son enteros positivos, y $n > 1$, entonces la representación*

$$m = a_k n^{k-1} + a_{k-1} n^{k-2} + \cdots + a_1$$

en donde $a_k \neq 0$, $0 \leq a_i < n$ para $i = 1, 2, \ldots, k$, existe para algún entero k y es única.

Por ejemplo, el entero 130, puede expresarse en bases 10, 2, 3, 4, 5 y 6, como sigue:

II-13. $130 = 1 \cdot 10^2 + 3 \cdot 10 + 0 = 130_{10}$,

$130 = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 = 10000010_2$,

$130 = 1 \cdot 3^4 + 1 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3 + 1 = 11211_3$,

$130 = 2 \cdot 4^3 + 0 \cdot 4^2 + 0 \cdot 4 + 2 = 2002_4$,

$130 = 1 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5 + 0 = 1010_5$,

II-14. $130 = 3 \cdot 6^2 + 3 \cdot 6 + 4 = 334_6$.

Los enteros a_i pueden encontrarse por medio de la aplicación repetida del Algoritmo de la División (Cap. II - 2), pero el procedimiento es completamente diferente del que se usó en el Cap. II - 5. Por ejemplo, en las expresiones anteriores (II - 13) y (II - 14), tenemos,

$$\begin{aligned} 130 &= 10 \cdot 13 + 0, \\ 13 &= 10 \cdot 1 + 3, \\ 1 &= 10 \cdot 0 + 1, \end{aligned} \qquad \begin{aligned} 130 &= 6 \cdot 21 + 4 \\ 21 &= 6 \cdot 3 + 3, \\ 3 &= 6 \cdot 0 + 3. \end{aligned}$$

Los restos sucesivos 0, 3, 1 cuando se divide 130 repetidas veces por 10, son las unidades, decenas y centenas representadas por los dígitos correspondientes, es decir, los coeficientes de 1, 10, y 10^2 en la fórmula (II - 13). Asimismo, los restos sucesivos 4, 3, 3 cuando 130 se divide reiteradamente por 6, son los coeficientes de 1, 6, y 6^2 en la expresión (II - 14). Estos coeficientes se obtienen fácilmente por medio de los siguientes esquemas donde los restos se separan a un lado:

$$\begin{array}{r|l} 10 & 130 \\ \hline 10 & 13 \sim 0 \\ 10 & 1 \sim 3 \\ 0 & \sim 1 \end{array} \qquad \begin{array}{r|l} 6 & 130 \\ \hline 6 & 21 \sim 4 \\ 6 & 3 \sim 3 \\ 0 & \sim 3 \end{array}$$

En general, el coeficiente a_i, del Teorema II - 13, puede obtenerse como sigue. Supongamos

$$\begin{aligned} m &= q_1 n + r_1, \\ q_1 &= q_2 n + r_2, \\ q_2 &= q_3 n + r_3, \\ &\cdots \\ &\cdots \\ q_{k-2} &= q_{k-1} n + r_{k-1}, \\ q_{k-1} &= 0 \cdot n + r_k, \end{aligned}$$

en donde $0 \leqq r_i < n$. De estas ecuaciones, se tienen $m > q_1 > q_2 > \cdots > q_{k-1} > 0$; $0 < q_{k-1} < n$; $r_k = q_{k-1}$, y por lo tanto $0 < r_k$. Los coeficientes del Teorema II - 13 se obtienen haciendo $a_k = r_k$, $a_{k-1} = r_{k-1}$, $\ldots$, $a_1 = r_1$.

Las relaciones $a_j = r_j$ pueden verificarse substituyendo cada q_i en la ecuación $q_{i-1} = q_i n + r_i$ para $i = k - 1, k - 2, \ldots, 2, 1$, y $q_0 = m$, como sigue:

$$q_{k-1} = r_k,$$
$$q_{k-2} = r_k n + r_{k-1},$$
$$q_{k-3} = r_k n^2 + r_{k-1} n + r_{k-2},$$
$$\cdot$$
$$\cdot$$
$$q_1 = r_k n^{k-2} + r_{k-1} n^{k-3} + \cdots + r_2,$$
$$m = r_k n^{k-1} + r_{k-1} n^{k-2} + \cdots + r_1.$$

Si hubiera dos expresiones para m en la misma base n, sean

$$m = a_0 n^k + a_1 n^{k-1} + \cdots + a_{k-1} n + a_k,\ 0 < a_0\ 0 \leqq a_i < n$$

y

$$m = b_0 n^p + b_1 n^{p-1} + \cdots + b_{p-1} n + b_p,\ 0 < b_0,\ 0 \leqq b_i < n,$$

entonces tendríamos

$$a_0 n^k + a_1 n^{k-1} + \cdots + a_k - (b_0 n^p + b_1 n^{p-1} + \cdots + b_p) = 0.$$

El miembro de la derecha, 0 (y por lo tanto el miembro de la izquierda de esta ecuación) es divisible por n. Por eso n es divisor de $a_k - b_p$. Pero

$$0 \leqq a_k < n,\ 0 \leqq b_p < n,\ |a_k - b_p| < n,$$

y n no es divisor de ningún entero positivo menor que n. Puesto que $|a_k - b_p|$ es divisible por n, no puede ser positivo y debe ser igual a 0, es decir, $a_k = b_p$. Asimismo, ambos miembros deben ser divisibles por n^{j+1}, de donde $a_{k-j} = b_{p-j}$ o, en general, $a_i = b_i$ para todos los valores de i, y tenemos que $p = k$. Por consiguiente la representación de m en el Teorema II - 13 es única.

La notación indo-arábica o sistema decimal (Cap. II-7) que nosotros usamos, consta de números expresados en base 10. En este caso el Teorema II - 3 establece que todo entero positivo tiene una representación única en base 10. Por ejemplo,

$$5604 = 5 \cdot 10^3 + 6 \cdot 10^2 + 0 \cdot 10 + 4.$$

Asimismo para $n = 2$ el Teorema II - 13 establece que todo entero positivo tiene una representación única en base 2. Por ejemplo,

$$183 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1,$$

y puede indicarse por 10110111_2. El sistema binario puede ampliarse de la misma manera que el sistema decimal para representar $7.625 = 1 \cdot 2^2 + 1 \cdot 2 + 1 \cdot 2^0 + 1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$ por 111.101_2. Sobre el sistema binario se basa la multiplicación campesina rusa, un antiguo método de convertir en suma la multiplicación de dos enteros (Ejercicios 11 y 12). Más recientemente, como se dijo antes, el sistema binario es la base de los cálculos con computadores electrónicos.

Hay muchos problemas y juegos que dependen de la escala de notación, es decir, de la base en la cual se expresan los números. Ball (Ver Bibliografía Nº 3; págs. 11 - 16) señala varios problemas en donde se utiliza la base 10. Por ejemplo, si una persona elige dos enteros menores que 10 (es posible al tirar dos dados), se puede descubrir cuáles son los enteros, pidiéndole lo siguiente:

(i) que elija uno de los enteros y lo multiplique por 5,
(ii) que sume 7,
(iii) que multiplique por 2,
(iv) que sume el segundo entero y le diga el resultado.

De la explicación algebraica de este procedimiento, queda claro que lo único que se necesita es sustraer 14 del número dado como resultado por la persona para obtener un número cuyos dos dígitos son precisamente los enteros en cuestión.

(i) $5a$,
(ii) $5a + 7$,
(iii) $10a + 14$,
(iv) $10a + 14 + b$.

El juego de Nim (Ver Bibliografía Nº 50; págs. 16-19) puede analizarse completamente mediante los números binarios. Otro juego relacionado con números binarios (Bibliografía Nº 43; pág. 39) necesita k tarjetas para el caso en que se consideran números menores que 2^k. Todos los enteros positivos menores que 2^k tienen un desarrollo único como suma de potencias de dos en la forma

(II - 15) $$n = a_1 + a_2 \cdot 2 + a_3 \cdot 2^2 + \ldots + a_k \cdot 2^{k-1},$$

en donde $a_i = 0$ ó 1 $(i = 1, 2, \ldots, k)$. La primera tarjeta contiene todos los enteros positivos menores que 2^k para los cuales $a_1 = 1$, la segunda aquéllos para los cuales $a_2 = 1$, ..., las de orden k aquellos para los cuales $a^k = 1$. El primer número de la j-ésima carta es 2^{j-1}. Por consiguiente, para determinar un número, sólo se necesita saber en qué tarjeta aparece, es decir, las potencias de 2 que se utilizaron en su desarrollo binario. Cualquier persona que se familiarice con el juego puede, entonces, decir el número sin mirar las tarjetas, puesto que se ha dado su representación como número binario. El número deseado es la suma de los primeros números en cada una de las tarjetas donde aparece. Por ejemplo, si $k = 4$, tenemos las tarjetas

1	9
3	11
5	13
7	15

2	10
3	11
6	14
7	15

4	12
5	13
6	14
7	15

8	12
9	13
10	14
11	15

El número $5 = 1 + 0 \cdot 2 + 1 \cdot 2^2$ aparece sólo en la primera y tercera tarjeta. El número que aparece sólo en la segunda y tercera tarjeta es $0 \cdot 2^0 + 1 \cdot 2 + 1 \cdot 2^2 = 6$. El número que aparece sólo en la primera, tercera y cuarta tarjetas es $1 \cdot 2^0 + 0 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 = 13$. En general, la representación binaria del número es conocida tan pronto como se conocen las tarjetas en las cuales aparece el número, en (II - 15) $a_1 = 1$ si el número n está en la primera tarjeta, $a_1 = 0$ si n no está en la primera tarjeta. Asimismo, considerando $n < 16$ o un conjunto mayor de tarjetas que las dadas anteriormente, $a_i = 1$ en (II - 15) si n está en la tarjeta de orden i, de otro modo $a_i = 0$.

EJERCICIOS

1. Expresar 19 y 175 en base 2.
2. Expresar 95 y 348 en base 3.
3. Expresar 75 y 6789 en base 7.
4. En cada uno de los ejercicios anteriores, sumar los dos números usando la base nueva. Comprobar la adición sumando los dos números tal como se dieron en la base diez y expresando la suma en la base indicada.

5. Repetir el Ejercicio 4 efectuando la sustracción del segundo número menos el primero, en lugar de la adición.

6. Repetir el Ejercicio 4, efectuando la multiplicación.

7. Repetir el Ejercicio 4, efectuando la división del segundo número por el primero.

8. Expresar el número 12143_5 (el subíndice indica la base) en base 10 y en seguida en base 7.

9. Expresar 12143_6 en base 7 sin cambiarlo a base 10.

10. Proponer un método general para cambiar la base de cualquier entero. Ilustrar el método propuesto con tres enteros de por lo menos cinco dígitos cada uno y en donde todas las bases sean diferentes de diez.

11. Damos el siguiente ejemplo de la multiplicación campesina rusa de $43 \cdot 75$. Las partes enteras de los cuocientes sucesivos de 43 dividido por 2 están alineadas al lado de los múltiplos sucesivos de 75 multiplicado por 2. En seguida aquellos múltiplos de 75 que corresponden a cuocientes impares de 43 se suman para obtener el producto pedido.

43	75
21	150
(10)	(300)
5	600
(2)	(1200)
1	2400

$43 \cdot 75 = 75 + 150 + 600 + 2400 = 3225$. Representar en el sistema binario y proponer una demostración de la validez de este método.

12. Encontrar los siguientes productos por medio de la multiplicación campesina rusa $67 \cdot 85$; $73 \cdot 120$; $121 \cdot 373$.

13. La simplificación siguiente $\frac{16}{64}$ ofrece una respuesta correcta para la fracción $\frac{16}{64}$ en base diez. Encontrar, en base diez, todas las fracciones m/n, en donde $10 < m < 20$, y $10 < n < 100$, tales que después de efectuarse simplificaciones semejantes a la del Ejercicio 13, den una respuesta correcta.

14. Encontrar todas las fracciones m/n tales que m, n sean números de dos dígitos en base diez y que al simplificar como en el Ejercicio 13, resulte una respuesta correcta.

15. Demostrar que no hay fracciones como las que se piden en el Ejercicio 14, si los números se expresan en base p, en que p es un número primo.

II-7 NOTACION DECIMAL. La representación de un número en base 10 se llama *notación decimal* del número. En el Capítulo II - 6 hemos encontrado que cualquier entero positivo m tiene una representación única en la notación decimal, es decir,

$$m = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0,$$

en donde

$$\begin{aligned} m &= 10\, m_1 + a_0 \\ m_1 &= 10\, m_2 + a_1 \\ &\cdot \\ &\cdot \\ &\cdot \\ m_k &= 10 \cdot 0 + a_k \end{aligned}$$

y $0 \leqq a_j < 10$, $a_k \neq 0$.

Consideraremos ahora la representación en la notación decimal de los números racionales positivos s/n. Esta representación también está basada en el Algoritmo de la División. Por ejemplo, dado el número $51/8$, podemos calcular

$$\begin{aligned} 51 &= 6 \cdot 8 + 3, \\ 30 &= 3 \cdot 8 + 6, \\ 60 &= 7 \cdot 8 + 4, \\ 40 &= 5 \cdot 8 + 0, \end{aligned}$$

y escribir $51/8 = 6.3750$. En general, dado cualquier número racional positivo s/n, podemos usar el Algoritmo de la División y escribir

$$s = mn + r,$$

en donde $0 \leqq m$ y $0 \leqq r < n$. El entero positivo m tiene un desarrollo decimal como en el caso anterior. El dígito de los décimos en el desarrollo decimal de r/n, y por lo tanto de s/n, es b_1, en que

$$10r = b_1 n + r_1,\ 0 \leqq r_1 < n.$$

El dígito de los centésimos es b_2, en que

$$10r_1 = b_2 n + r_2,\ 0 \leqq r_2 < n$$

y en general, para cualquier entero positivo j, el dígito j-ésimo hacia la derecha del punto decimal en el desarrollo de s/n es b_j, en donde

$$10r_{j-1} = b_j n + r_j,\ 0 \leqq r_j < n.$$

Queda por demostrar que se necesita únicamente un número finito de estas etapas para obtener la representación de s/n en la notación decimal.

En realidad, existe un conjunto infinito numerable de restos r_j $(j = 1, 2, \ldots)$ tal que $0 \leqq r_j < n$. Sin embargo, puesto que cada r_j es un elemento del conjunto 0, 1, 2, ..., $n - 1$, hay solamente un número finito de valores distintos de los restos r_j. En efecto, deben existir enteros p, y $q = p + t$, en que t es positivo, tales que $r_{p-1} = r_{q-1}$, y por lo tanto

$$nb_p + r_p = nb_q + r_q,$$
$$n(b_p - b_q) = r_q - r_p$$

Puesto que los enteros positivos son bien ordenados, existen enteros positivos mínimos p y t que tienen las propiedades anteriores. Cualquier $p_1 > p$ y cualquier entero positivo múltiplo de t también tiene estas propiedades. Si $b_p = b_q$, entonces $r_q = r_p$. Si $b_p \neq b_q$, entonces n es divisor de $r_q - r_p$, en que $0 \leqq r_q < n$, $0 \leqq r_p < n$, y por lo tanto $r_q - r_p = 0 = b_p - b_q$, contrariamente a nuestra creencia de que $b_p \neq b_q$, tenemos que $b_p = b_q$ y $r_p = r_q$. De este modo hemos demostrado que existen enteros positivos diferentes p, q tales que $r_{p-1} = r_{q-1}$ y que esta igualdad implica $r_p = r_q$, es decir, $r_p = r_{p+t}$, en donde $q = p + t$. Finalmente, según el principio de inducción matemática, $r_j = r_{j+t}$ para todos los $j \geqq p - 1$ y el número positivo racional s/n puede escribirse en la forma:

$$a_k 10^k + \cdots + a_1 10 + a_0 + \frac{b_1}{10} + \frac{b_2}{10^2} + \cdots + \frac{b_p}{10^{p-1}} + \frac{c_1}{10^p} + \frac{c_2}{10^{p+1}} + \cdots$$

$$+ \frac{c_t}{10^{p+t-1}} + \frac{c_1}{10^{p+t}} + \frac{c_2}{10^{p+t+1}} + \cdots + \frac{c_t}{10^{p+2t-1}} + \frac{c_1}{10^{p+2t}} + \cdots$$

Hemos hecho una demostración completa de que todo número racional positivo puede representarse por un decimal periódico. En la práctica, como en la teoría, se procede como se hizo anteriormente para encontrar los r_j hasta que algún r_j sea cero, o sea, igual a algún r_k, en donde $k < j$. Por ejemplo, dado 153/7, se calcula

$$\begin{aligned} 153 &= 21 \cdot 7 + 6 \\ 60 &= 8 \cdot 7 + 4 \\ 40 &= 5 \cdot 7 + 5 \\ 50 &= 7 \cdot 7 + 1 \\ 10 &= 1 \cdot 7 + 3 \\ 30 &= 4 \cdot 7 + 2 \\ 20 &= 2 \cdot 7 + 6, \end{aligned}$$

de donde $153/7 = 21.857142857142\ldots$ Puesto que los decimales precedidos de signo se emplean para representar números precedidos de signo, todos los números racionales pueden representarse como fracciones periódicas. Recíprocamente, dado cualquier decimal d en el que se repiten una y otra vez t dígitos, podemos calcular el decimal finito $10^t d - d$ (Cap. I - 10) y expresar d como un número racional. De esta manera hemos demostrado que todo número racional puede expresarse como un decimal periódico, y viceversa. Los temas que siguen de este capítulo son importantes para la teoría de los números pero pueden suprimirse sin perturbar la organización de este texto.

EJERCICIOS

1. Emplear el método anterior de restos sucesivos y expresar cada uno de los siguientes números racionales en notación decimal:

$$\frac{1}{16}, \quad \frac{1}{50}, \quad \frac{3}{11}, \quad \frac{2}{3}, \quad \frac{1}{10}, \quad \frac{1}{128}.$$

2. Repetir el Ejercicio 1 para $\frac{17}{3}$, $\frac{25}{8}$, $\frac{11}{6}$, $\frac{75}{16}$, $\frac{125}{36}$.

3. Demostrar que todo número racional puede representarse como un decimal periódico, valiéndose de que se obtienen a lo más q restos diferentes de los cuocientes $10^j/q$, en donde $j = 0, 1, 2, \ldots$.

4. Examinar el caso de la representación de números racionales en el sistema binario de números.

II-8* **CONGRUENCIAS.** Procederemos ahora a dividir el conjunto de los enteros en subconjuntos o subclases respecto a un entero m dado elegido arbitrariamente. Por ejemplo, de aquí a tres horas, de aquí a cincuenta y una horas, hace veintiuna horas, y, en general, $3 + 24k$ horas de ahora en adelante para cualquier entero k, todos representan la misma hora del día. Los números de horas, 3, 51, -21, $3 + 24k$ son equivalentes en cierto sentido respecto a un día de veinticuatro horas. Se dice que los números son congruentes módulo 24 y se escribe $3 \equiv 51$ (mód. 24). Asimismo, ángulos de 30°, 390°, $-330°$, 750°, y en general, $30° + (360k)°$ para cualquier entero k pueden representarse gráficamente utilizando los mismos lados inicial y terminal. Además, siempre que ángulos de $a°$ y de $b°$ puedan representarse utilizando los mismos lados inicial y terminal, tenemos que $a = b + 360\ k$ para algún entero k y se puede escribir $a \equiv b$ (mód. 360). En general se dice que dos enteros a y b son *congruentes módulo un entero* m si y sólo si existe un entero c que satisfaga la igualdad $a = b + cm$. Todas las veces que tal entero c exista, podemos escribir $a \equiv b$ (mód. m) y llamar a m el *módulo* de la congruencia. Esta definición es equivalente a la relación $a \equiv b$ (mód. m) si y sólo si $a - b$ es divisible por m. Por ejemplo $3 \equiv 8$ (mód. 5), $-3 \equiv 9$ (mód. 6), y dos enteros pares cualesquiera son congruentes módulo 2.

La congruencia módulo m es una relación de equivalencia (Cap. 1-3), dado que es reflexiva, simétrica, y transitiva, es decir,

(i) $a \equiv a$ (mód. m),
(ii) $a \equiv b$ (mód. m) implica $b \equiv a$ (mód. m), y
(iii) $a \equiv b$ (mód. m) y $b \equiv c$ (mód. m) implican $a \equiv c$ (mód. m).

Es fácil demostrar estas tres propiedades basándose en las definiciones ya citadas: $a = a + 0m$; si $a = b + km$, entonces $b = a + (-k)m$; si $a = b + km$ y $b = c + hm$, entonces $a = c + (h + k)m$. La relación de equivalencia $=$ puede considerarse como un caso especial de $\equiv$, en que el $m = 0$. Sin embargo, en nuestro estudio nosotros vamos a admitir que $m \neq 0$.

Consideraremos en seguida algunas de las propiedades de esta nueva relación $\equiv$ (mód. m). Las congruencias módulo m pueden

combinarse empleando las operaciones del anillo: adición, sustracción, y multiplicación, es decir, si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces,

$$(\text{II} - 16) \qquad a + c \equiv b + d \pmod{m},$$
$$(\text{II} - 17) \qquad a - c \equiv b - d \pmod{m},$$
$$(\text{II} - 18) \qquad ac \equiv bd \pmod{m}.$$

Estas congruencias pueden demostrarse directamente basándose sobre la definición de congruencia. Si $a = b + sm$ y $c = d + tm$, entonces

$$a + c = b + d + (s + t)m,$$
$$a - c = b - d + (s - t)m,$$
$$\text{y} \quad ac = bd + (bt + sd + stm)m,$$

en que $s + t$, $s - t$, y $bt + sd + stm$ son enteros, ya que el conjunto de los enteros es cerrado con respecto a las operaciones del anillo. La congruencia (II - 18) puede aplicarse para el caso especial de que $a = c$, $b = d$ y, por inducción matemática, resulta para cualquier entero positivo n

$$(\text{II} - 19) \qquad a^n \equiv b^n \pmod{m}.$$

Por ejemplo las congruencias $2 \equiv 7 \pmod{5}$ y $3 \equiv 8 \pmod{5}$ pueden sumarse y resulta $5 \equiv 15 \pmod{5}$; pueden restarse y se obtiene $-1 \equiv -1 \pmod{5}$; y multiplicarse para obtener $6 \equiv 56 \pmod{5}$. También se puede elevar al cuadrado ambos miembros de la congruencia $2 \equiv 7 \pmod{5}$ y se obtiene $4 \equiv 49 \pmod{5}$.

Dado que para la formación de un polinomio sólo se necesitan operaciones anillo (Cap. III - 2), pueden aprovecharse las congruencias (II - 16), (II - 17), (II - 18), (II - 19) para obtener

TEOREMA II - 14. *Si $a \equiv b \pmod{m}$ y $f(x)$ es un polinomio con coeficientes enteros, entonces $f(a) \equiv f(b) \pmod{m}$.*

Consideremos como un ejemplo de este teorema al polinomio $f(x) = x^3 - 3x^2 + 2x + 1$ y a la congruencia $2 \equiv -1 \pmod{3}$, $f(2) = 8 - 12 + 4 + 1 = 1$ y $f(-1) = -1 - 3 - 2 + 1 = -5 \equiv 1 \pmod{3}$.

También rige la ley cancelativa para las congruencias. Si $ak \equiv bk$ (mód. m), su diferencia es un múltiplo de m, es decir $(a - b)k = tm$. Sea $d = (k, m)$, entonces

$$(a - b)k/d = t(m/d) \text{ y } a \equiv b \text{ (mód. } m/d).$$

Por ejemplo, $2 \equiv 8$ (mód. 6) implica $1 \equiv 4$ (mód. 3); $12 \equiv 32$ (mód. 10) implica $6 \equiv 16$ (mód. 5) y $3 \equiv 8$ (mód. 5). Si $ak \equiv bk$ (mód. m) y $(k, m) = 1$, entonces $a \equiv b$ (mód. m). En general, se tiene.

TEOREMA II-15. *Si* $ak \equiv bk$ (mód. m) y $(k, m) = d$, *entonces* $a \equiv b$ (mód. m_1), *en que* $m = dm_1$.

Las congruencias pueden servir para dar pruebas de la divisibilidad de cualquier entero n por un entero m. Todo entero positivo puede expresarse unívocamente (Cap. II-6), en la forma (II-20)

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_k \cdot 10^k, \tag{II-20}$$

en donde $0 \leq a_i \leq 9$ siendo $i = 1, 2, \ldots, k$. La prueba tan familiar para la divisibilidad por 2 se encuentra considerando ambos miembros de (II-20) con respecto al módulo 2. Dado que $10 \equiv 0$ (mód. 2), podemos reemplazar 10, 10^2, ..., y 10^k por 0 en el caso de que se considere a n en (II-20) con respecto al módulo 2. Luego $n \equiv a_0$ (mód. 2), es decir, $n = a_0 + 2t$ para cualquier entero t, y n es divisible por 2 si y sólo si a_0 es divisible por 2. Asimismo, de $10 \equiv 1$ (mód. 3) y de la relación (II-19), se tiene $n \equiv a_0 + a_1 + \ldots + a_k$ (mód. 3), es decir, n es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3. Puesto que $10^2 \equiv 0$ (mód. 4), se obtiene $n \equiv a_0 + 10a_1$ (mód. 4), en donde n es divisible por 4 si y sólo si el número compuesto por sus últimos dos dígitos es divisible por 4. También se puede usar (II-20) para obtener:

$$\begin{aligned}
&n \equiv a_0 \pmod 5,\\
&n \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6\\
&\qquad + 3a_7 + 2a_8 - a_9 - \cdots \pmod 7,\\
&n \equiv a_0 + a_1 + \cdots + a_k \pmod 9,\\
&n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k \pmod{11},\\
&n \equiv a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5 + a_6\\
&\qquad - 3a_7 - 4a_8 - a_9 + \cdots \pmod{13},\\
&n \equiv a_0 + 10a_1 \pmod{25},
\end{aligned} \tag{2-21}$$

y muchas otras pruebas semejantes para la divisibilidad. Por ejemplo, $342538 \equiv 0 \pmod 7$, es decir, es divisible por 7, dado que $a_0 = 8$, $a_1 = 3$, $a_2 = 5$, $a_3 = 2$, $a_4 = 4$, $a_5 = 3$, y empleando la prueba que acabamos de señalar, $342538 \equiv 8 + 3 \cdot 3 + 2 \cdot 5 - 2 - 3 \cdot 4 - 2 \cdot 3 = 7 \equiv 0 \pmod 7$. De manera análoga, 3637425 es divisible por 11, y 7587125 es divisible por 13. La naturaleza periódica de los múltiplos de los dígitos a_i se examina en los Ejercicios 5 y 6, Cap. II-10.

Antes de la invención de la máquina de calcular, se revisaban muchos procedimientos aritméticos por el método de *calcular los nueves*, es decir, se consideraban los números con respecto al módulo 9 como en (II-21) y se empleaban las congruencias (II-16), (II-17), y (II-18). El producto $321 \cdot 152 = 48792$ se revisaría por medio de las congruencias $321 \equiv 6 \pmod 9$, $152 \equiv 8 \pmod 9$, $321 \cdot 152 \equiv 6 \cdot 8 \equiv 48 \equiv 3 \equiv 48792 \pmod 9$. Este método no es una revisión perfecta, ya que no se localizan algunos errores, como por ejemplo, el intercambio de dos dígitos. En el caso de un cuociente $a/b = q + r/b$, la relación $a = qb + r$ debe ser válida y se comprueba que $a \equiv qb + r \pmod 9$. Por ejemplo, la ecuación $\frac{83}{17} = 4 + \frac{15}{17}$ se comprueba considerando que $83 = 4 \cdot 17 + 15$, lo que resulta $2 \equiv 4 \cdot (-1) + 6$ (módulo 9).

EJERCICIOS

1. Demostrar que $a^2 \equiv 1$ (módulo 8), en donde a es cualquier número impar.

2. Proponer cuatro ejemplos del Teorema II-14, usando polinomios de por lo menos tercer grado.

3. Encontrar $f(13) \pmod 9$ si $f(x) = 7x^3 + 13x^2 - 72x^2 + 2153$.

4. Proponer tres ejemplos numéricos que ilustren el Teorema II-15.

5. Proponer pruebas de la divisibilidad por 6, 8 y 15.

6. Examinar si 1113 y 23,535 son divisibles por 7, 9, 11 y 15 usando los teoremas de congruencia.

7. Comprobar lo siguiente por el método de "calcular los nueves":

   a) $1235 \cdot 341 = 421135$;
   b) $852 + 1239 + 251 + 172 = 2514$.

8. Exponer un método para "calcular los onces". Repetir el Ejercicio 7, calculando los onces.

9. Encontrar una demostración de la divisibilidad por 4, de números expresados en base cinco. Proponer un ejemplo de tres dígitos y otro de cuatro dígitos.

10. Proponer una demostración de la divisibilidad por $n - 1$ para números expresados en base n.

11. Proponer una demostración de la divisibilidad por $n + 1$ para números expresados en base n.

12. Proponer demostraciones de la divisibilidad por 4, 8 y 16 y demostrar que se necesitan considerar cuando más b dígitos para probar la divisibilidad por 2^b de cualquier entero dado expresado en base 10.

13. Demostrar que $a \equiv b$ (mód. m), $0 < a < m$, $0 < b < m$, implica $a = b$.

14. Tres hermanos decidieron en el colegio repartir su caja común de bolitas entre los siete miembros de su pandilla. El primero de los tres hermanos que llegó a su casa repartió las bolitas en siete grupos y le sobró una bolita, tomó su pila y la bolita sobrante. El segundo hermano, llegó a su casa, repartió las bolitas restantes en siete pilas, le sobró una bolita que dio a su hermana y tomó su pila. Cuando el tercer hermano llegó a su casa, separó las bolitas restantes exactamente en siete pilas iguales. Encontrar el menor número posible de bolitas para el número original de bolitas. Dar todas las soluciones considerando el problema como clase de congruencia (Cap. II-9). *(Indicación:* Comenzar expresando el número pedido en base 7, por ejemplo, $N = abc_7$).

II-9* CLASES RESIDUALES. FUNCION ϕ DE EULER. Dados dos enteros cualesquiera c y m, el Algoritmo de la División establece que existen enteros q y r, $0 \leq r < m$, tales que $c = qm + r$. El número r se llama el *residuo* de c con respecto al módulo m y se escribe $c \equiv r$ (mód. m). Por ejemplo, $7 \equiv 2$ (mód. 5), $31 \equiv 1$ (mód. 5), $102 \equiv 2$ (mód. 5). La totalidad de los números c tales que $c \equiv r$ (mód. m) se llama *clase residual o clase de congruencia* con respecto al módulo m y se indica por $[r]$ (mód. m). Los números de la clase $[r]$ (mód. m), son

$$r,\ r \pm m,\ r \pm 2m,\ r \pm 3m,\ \ldots.$$

Por ejemplo, la clase residual [2] (mód. 5), comprende a los números

$$\ldots,\ -13,\ -8,\ -3,\ 2,\ 7,\ 12,\ 17,\ \ldots.$$

Todo entero positivo, negativo o cero pertenece, con respecto al módulo 5, a una de las clases residuales [0], [1], [2], [3], [4] (mód. 5). En general, todo entero pertenece, con respecto al mó-

dulo m, a una de las clases residuales [0], [1], [2], . . . , [m—1] (mód. m) (ver Ejercicio 8). Para $m = 2$ todos los números pares pertenecen a la clase residual [0] (mód. 2) y todos los números impares pertenecen a la clase residual [1] (mód. 2). Un conjunto de números $r_1, r_2 \ldots r_m$, en que cada uno de ellos pertenece a cada una de las clases [0], [1], [2], . . . , [m—1] (mód. m), se llama un *sistema residual completo*, con respecto al módulo m. Por ejemplo, los números 5 y 8 forman un sistema residual completo con respecto al módulo 2; los números 64, 17, 34, y —1 forman un sistema residual completo con respecto al módulo 4.

Una clase residual [r] (mód. m) puede ser expresada en función de cualquiera de sus elementos, es decir, [r] (mód. m) = [$r + km$] (mód. m) para cualquier entero k. De este modo, para cualquier entero m el número total de clases residuales distintas con respecto al módulo m es $|m|$. Un conjunto de números $r_1, r_2, \ldots, r_m$ es un sistema residual completo con respecto al módulo m si y sólo si $r_i \not\equiv r_j$ (mód. m) siempre que $i \neq j$ e $i, j = 1, 2, \ldots, m$.

Los sistemas residuales completos pueden usarse en la determinación de todas las raíces n-ésimas de la unidad a partir de una raíz n-ésima primitiva dada de la unidad. Por definición (Cap. I-17), s es una raíz n-ésima de la unidad si y sólo si n es el entero positivo menor k tal que $s^k = 1$. Luego si $s^m = 1$, podemos escribir $m = qn + r$, en donde $0 \leq r < n$, y obtener $s^m = s^{qn+r} = s^{qn} \cdot s^r = s^r = 1$. Ahora, dado que $0 \leq r < n$, $s^r = 1$ y n es el menor entero positivo k tal que $s^k = 1$, tenemos que $r = 0$ y $m = qn$, es decir, $s^m = 1$ si y sólo si $m \equiv 0$ (mód. n), en donde s es una n-ésima raíz primitiva de la unidad.

El Teorema de De Moivre (Cap. I-17) establece la existencia de por lo menos una raíz n-ésima primitiva de la unidad para cualquier entero positivo n. Dada una raíz s n-ésima primitiva de la unidad, resulta que, según (Cap. I-17), toda potencia entera de s, por ejemplo, s^t, era también una raíz n-ésima, dado que $(s^t)^n = (s^n)^t = 1^t = 1$. Además, si $s^t = s^u$, entonces $s^{t-u} = 1$ y $t - u \equiv 0$ (mód. n), es decir, $t \equiv u$ (mód. n). De aquí que dos potencias enteras de una raíz n-ésima primitiva de la unidad sean distintas si y sólo si los exponentes pertenecen a distintas clases residuales con respecto al módulo n. Después de esto, podemos generalizar el Teorema I-7, como sigue:

TEOREMA II-16. *Todas las n-ésimas raíces de la unidad están dadas por la sucesión*

$$s^{r_1}, s^{r_2}, \ldots, s^{r_n},$$

en donde s es una raíz n-ésima primitiva de la unidad y los r_i forman un sistema residual completo respecto al módulo n.

Por ejemplo, si $n = 4$, entonces 16, -11, 30, 67 forman un sistema residual completo y todas las raíces cuartas de la unidad pertenecen al conjunto $i^{16} = 1$, $i^{-11} = i$, $i^{30} = -1$, $i^{67} = -i$, en donde $i = \sqrt{-1}$.

Definiremos, en seguida, un segundo tipo de sistema residual, llamado sistema residual reducido.

El número de enteros positivos menores que o iguales a m y primos respecto de m, se denota por $\phi(m)$ para cualquier entero positivo m y se llama el indicador (totient) de m o *función ϕ de m de Euler*. Por eso, $\phi(m)$ es el número de enteros k del conjunto

$$1, 2, 3, \ldots, m-1, m \qquad \text{(II-22)}$$

tal que $(k, m) = 1$; $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, ... De lo anterior y de la definición de números primos entre sí (Cap. II-1), se obtiene $\phi(1) = 1$.

Si $(r, m) = 1$, entonces para cualquier entero k tenemos $(r + km, m) = 1$, es decir, todo elemento de $[r]$ (mód. m) es un número primo con respecto a m. Por consiguiente, una clase residual $[r]$ (mód. m) es *prima respecto de m* si y sólo si $(r, m) = 1$. Utilizaremos estas relaciones para definir un sistema residual reducido. Un conjunto de números $r_1, r_2 \ldots, r_{\phi(m)}$, en que cada uno de ellos pertenece a cada una de las clases residuales que son primas respecto de m, se llama un *sistema residual reducido* respecto del módulo m.

Este segundo tipo de sistema residual puede emplearse también en el estudio de las n-ésimas raíces de la unidad. Supongamos que s es una raíz n-ésima primitiva de la unidad, y consideremos que k sea tal que s^k sea una raíz n-ésima primitiva de la unidad. Entonces $(s^k)^n = 1$ para cualquier entero k, dado que s es una raíz n-ésima primitiva. Si $(k, n) = d > 1$, entonces $k = k_1 d$, $n = n_1 d$, en donde $n_1 < n$ y $(s^k)^{n_1} = (s^{k_1 d})^{n_1} = (s^{n_1 d})^{k_1} = 1^{k_1} = 1$, es decir,

s^k no es una raíz n-ésima primitiva si $(k, n) = d > 1$. Si $(k, n) = 1$ y $(s^k)^m = 1$, entonces $km \equiv 0$ (mód. n); es decir, $n \mid km$ y, según el Teorema II-9, $n \mid m$, de donde s^k es una raíz n-ésima primitiva de la unidad. Por consiguiente, s^k es una raíz n-ésima primitiva de la unidad si y sólo si $(k, n) = 1$. Esto nos permite encontrar todas las raíces n-ésimas primitivas dada una raíz n-ésima primitiva de la unidad.

TEOREMA II-17. *Si s es una raíz n-ésima primitiva de la unidad, entonces todas las raíces n-ésimas primitivas de la unidad pertenecen al conjunto*

$$s^{r_1}, s^{r_2}, \ldots, s^{r_{\phi(n)}},$$

en donde las r forman un sistema residual reducido con respecto al módulo n.

Usaremos también los sistemas residuales reducidos en las demostraciones del Teorema de Euler y del Teorema Simple de Fermat en la sección 10 de este Capítulo II.

EJERCICIOS

1. Escribir los sistemas residuales completos con respecto a los siguientes módulos enteros: 4, 5, 9, 11 y 16.

2. Escribir los sistemas residuales reducidos con respecto a los siguientes módulos enteros: 4, 5, 9, 11, 16, 31, 60, −70.

3. Demostrar que los números −5, −2, 12, 26, 39, 53 forman un sistema residual completo respecto al módulo 6.

4. Demostrar que m enteros consecutivos cualesquiera forman un sistema residual completo respecto al módulo m.

5. Demostrar que si $(d, m) = 1$, entonces $d, 2d, 3d, \ldots, md$ forman un sistema residual completo respecto al módulo m.

6. Demostrar que $a + r_1, a + r_2, a + r_3, \ldots, a + r_m$ es un sistema residual completo respecto al módulo m para cualquier entero a si $r_1, r_2, r_3, \ldots, r_m$ es un sistema residual completo respecto al módulo m.

7. Expresar un sistema residual completo respecto al módulo mn en que $(m, n) = 1$ en función de sistemas residuales completos dados de m y n.

8. Por medio del Algoritmo de la División demostrar que todo entero pertenece, respecto al módulo m, a una y solo una de las clases residuales [0], [1], ..., $[m - 1]$ (mód. m) en donde $m \neq 0$ es un entero arbitrario.

9. Definir $[a] + [b] = [a + b]$ respecto al módulo m; $[a] \cdot [b] = [ab]$ con respecto al módulo m, y demostrar que estas definiciones son independientes de los elementos particulares a, b elegidos de las clases residuales $[a]$, $[b]$ respecto al módulo m.

10. Demostrar que las clases residuales, módulo 5, forman un anillo.

11. Demostrar que las clases residuales, módulo 6, forman un anillo.

12. Demostrar que las clases residuales, módulo m para cualquier entero $m \neq 0$ forman un anillo.

13. Ilustrar el concepto de divisores cero (Cap. I-14) por medio de clases residuales respecto al módulo 6.

14. Demostrar que las clases residuales, módulo 5, forman un campo.

15. Demostrar que las clases residuales módulo p para cualquier número primo p forman un campo.

II-10* EVALUACION DE $\phi\ (m)$. Dado que todo entero positivo puede expresarse de una manera única como el producto de números primos (Teorema II-8) evaluaremos primero la función ϕ para los números primos. Si m es un número primo, entonces todo número, excepto m, en la relación (II-22) es primo respecto de m y $\phi\ (m) = m - 1$. Si $m = p^a$, en que p es un número primo, entonces en el conjunto 1, 2, 3, ..., p, $p + 1$, ..., $2p$, $2p + 1$, ..., $3p$, ..., p^a, sólo los números p, $2p$, $3p$, ..., $(p^{a-1})p$ son divisibles por p. Por consiguiente, $p^a - p^{a-1}$ de los números son primos respecto de p (Teorema II-5) y

$$\phi(p^a) = p^a\left(1 - \frac{1}{p}\right).$$

Demostraremos, en seguida, que si $m = uv$, en que $(u, v) = 1$, entonces $\phi\ (m) = \phi\ (u)\ \phi\ (v)$ y, en general, la función ϕ de un producto de factores primos entre sí, es igual al producto de las funciones ϕ de los factores. Esto puede demostrarse rápidamente teniendo en cuenta que hay exactamente $\phi\ (m)$ raíces m-ésimas primitivas de la unidad y que todas las raíces m-ésimas de la unidad forman un grupo cíclico (Cap. I-17). Se obtiene una demostración más larga, pero más elemental, escribiendo todos los enteros 1, 2, 3, ..., uv en una ordenación rectangular, como sigue:

1	2	3	...	h	...	u
$u+1$	$u+2$	$u+3$	...	$u+h$	...	$2u$
$2u+1$	$2u+2$	$2u+3$	...	$2u+h$	...	$3u$
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
$(v-1)u+1$	$(v-1)u+2$	$(v-1)u+3$	...	$(v-1)u+h$	...	vu.

Por ejemplo, si $u = 5$ y $v = 3$, se escribe:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15

Cada hilera forma un sistema residual completo respecto al módulo u. Cada columna forma parte de una sola clase residual (mód. u), es decir, todo elemento de la columna encabezada por el número h pertenece a $[h]$ (mód. u). Siendo así, los elementos de la columna encabezada por h son primos respecto de u, si y sólo si $(h, u) = 1$. El número de columnas cuyos elementos son primos respecto de u es, por lo tanto, $\phi(u)$. Demostraremos, en seguida, que en cada columna no hay dos elementos que pertenezcan a la misma clase residual respecto del módulo v. Consideremos $su + h$ y $tu + h$. Según el Algoritmo de la División,

$$su + h = q_s v + r_s, \quad 0 \leqq r_s < v,$$
$$tu + h = q_t v + r_t, \quad 0 \leqq r_t < v.$$

Supongamos que $r_s = r_t$, entonces $(s - t)u = (q_s - q_t)v$. Puesto que $(u, v) = 1$ y $u > 0$, o bien $q_s = q_t$ o bien v es divisor de $s - t$. Pero $s < v$, $t < v$ y según el Ejercicio 3, Cap. II - 1, se tiene $s = t$, es decir, no hay dos elementos distintos de ninguna columna determinada que sean congruentes respecto al módulo v. Ya que hay v elementos en cada columna, cada columna constituye un sistema residual completo respecto al módulo v y contiene exactamente $\phi(v)$ elementos que son primos respecto de v. Por consiguiente, en cada una de las $\phi(u)$ columnas de elementos primos respecto de u, hay $\phi(v)$ elementos que también son primos respecto de v, es decir, hay $\phi(u)\,\phi(v)$ elementos primos respecto de u y de v simultáneamente y, por consiguiente respecto de uv (Teorema II - 9). En

otras palabras, $\phi\,(uv) = \phi\,(u)\,\phi\,(v)$. En general, si $m_1, m_2, \ldots, m_k$ son k enteros positivos que son primos entre sí, entonces

$$\phi\,(m_1 m_2 \ldots m_k) = \phi\,(m_1)\,\phi\,(m_2) \ldots \phi\,(m_k).$$

De los dos últimos párrafos y del Teorema II - 8, resulta

TEOREMA II - 18. *Para cualquier entero positivo* $m = p_1^{a_1} \cdot p_2^{a_2} \ldots p_n a_n$, *en que los p son números primos distintos,*

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right).$$

Por ejemplo: $\phi(15) = 15(1 - \frac{1}{5})(1 - \frac{1}{3}) = 8$

o también $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8.$

Tenemos también el

TEOREMA II - 19. *Dados enteros positivos m, n, d, tales que* $m = nd$, *el número de enteros* $k \leqq m$ *tal que* $(k, m) = d$, *es* $\phi\,(n)$.

Esto se demuestra fácilmente, ya que todo número $\leqq m = nd$ que tenga un divisor d es uno del conjunto $d, 2d, 3d, td, \ldots, (n - 1)d, nd$ y $(td, m) = d$ o también $(td, nd) = d$ si y sólo si $(t, n) = 1$. Por consiguiente, el número de valores de t, tales que $(td, m) = d$ es exactamente $\phi\,(n)$.

El valor de $\phi\,(m)$ para cualquier entero positivo m puede encontrarse por medio del Teorema II - 18. Para $m \leqq 10{,}000$ estos valores se encuentran en un conjunto de tablas cuyo autor es J. W. L. Glaisher.

El siguiente teorema proporciona una aplicación muy importante de la función ϕ (ver Bibliografía Nº 43; págs. 272-310).

TEOREMA II - 20. TEOREMA DE EULER. *Si m es un entero positivo y a es cualquier entero tal que* $(a, m) = 1$, *entonces* $a^{\phi(m)} \equiv 1$ *(mód. m).*

Si m es un número primo p, este teorema se convierte en el Teorema formulado con anterioridad, por Fermat.

TEOREMA II - 21. TEOREMA SIMPLE DE FERMAT. *Si p es un número primo y* $p + a$, *entonces* $a^{p-1} \equiv 1$ (mód. p).

El Teorema II - 21 se expresa con frecuencia en la forma $a^p \equiv a$ (mód. p) que es válida para todos los enteros positivos a.

Una demostración del Teorema II - 20 y por lo tanto también del Teorema II - 21, supone un sistema residual reducido con respecto al módulo m, por ejemplo $r_1, r_2, \ldots, r_{\phi(m)}$. Dado que por hipótesis $(a, m) = 1$, el conjunto de elementos $ar_1, ar_2 \ldots, ar_{\phi(m)}$ también constituye un sistema residual reducido respecto al módulo m. Por lo tanto, los elementos de los dos sistemas deben ser congruentes módulo m en pares (siguiendo alguna ordenación) y por medio de la aplicación repetida de la relación (II - 18), tenemos

$$a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m}.$$

Por definición de un sistema residual reducido $(r_i, m) = 1$, en que $i = 1, 2, \ldots \phi(m)$. Siendo así, según el Teorema II - 15, podemos dividir ambos miembros de la ecuación anterior por $r_1 r_2 \ldots r_{\phi(m)}$ y obtenemos $a^{\phi(m)} \equiv 1 \pmod{m}$. Con esto se completa nuestra demostración del Teorema II - 20 y también del Teorema II - 21. En las dos últimas partes de este capítulo estudiaremos congruencias lineales y problemas diofánticos.

EJERCICIOS

1. Encontrar $\phi(12)$, $\phi(32)$, $\phi(17)$, $\phi(31)$, $\phi(60)$.
2. Demostrar que $(n-1)! \equiv 0 \pmod{n}$, en donde n es cualquier número compuesto diferente de 4.
3. Demostrar que $(a+b)^p \equiv a^p + b^p \pmod{p}$, en donde a y b son enteros cualesquiera y p es cualquier número primo.
4. Verificar el Teorema de Euler para $a = 7$ y $m = 12$.
5. Si $(m, 10) = 1$, demostrar que en la prueba para la divisibilidad por m de cualquier número suficientemente grande expresado en base 10, los múltiplos de los dígitos deben aparecer en conjuntos muy parecidos a los dígitos de un decimal periódico. Por ejemplo, $10^2 \equiv 1 \pmod{11}$ y $n \equiv a_0 - a_1 + a_2 - a_3 + \ldots \pmod{11}$, donde los múltiplos son el conjunto $+1, -1$ repetido hasta que se hayan considerado todos los dígitos del número dado.
6. Si $(m, 10) \neq 1$, hacer $m = 2^a 5^b n$ y valiéndose del Ejercicio 3, Cap. II-7, demostrar que para cualquier número m suficientemente grande, los múltiplos de los dígitos aparecen en conjuntos que se repiten después de haber considerado cierto número finito de dígitos.

II - 11* CONGRUENCIAS LINEALES. La aritmética se preocupa principalmente de números. En álgebra se introducen nuevos símbolos llamados *variables* (Cap. III - 1).

Ahora nos apartaremos momentáneamente de la aritmética y volveremos al álgebra. Según la teoría de las ecuaciones, podemos considerar el problema de encontrar enteros x que satisfagan una congruencia de polinomios $f(x) \equiv 0 \pmod{m}$. Si a es un entero tal que $f(a) \equiv 0 \pmod{m}$ y $a \equiv b \pmod{m}$, entonces, según el Teorema II - 14, tenemos $f(b) \equiv 0 \pmod{m}$ y existe un conjunto de enteros infinito numerable

$$a,\ a \pm m,\ a \pm 2m,\ a \pm 3m,\ \ldots$$

que satisface la congruencia $f(x) \equiv 0 \pmod{m}$. Se habla de la clase residual completa $[a] \pmod{m}$ como la única *solución* de la congruencia de polinomios. De esta manera el número de soluciones de $f(x) \equiv 0 \pmod{m}$ es el número de clases residuales $[r_1]$, $[r_2]$, $\ldots$, $[r_k] \pmod{m}$ tales que $f(r_i) \equiv 0 \pmod{m}$. Dado que existen exactamente m clases residuales distintas, cualquier congruencia de polinomios dada tiene máximo m soluciones respecto al módulo m.

En el anillo de los enteros, puede dividirse ambos miembros de la ecuación $ax = b$ (Cap. II - 1) por a si y sólo si existe un entero c tal que $ac = b$. De manera análoga, la divisibilidad de ambos miembros de una congruencia respecto al módulo m por un entero se relaciona con la solución de una congruencia lineal $ax \equiv b \pmod{m}$. Por consiguiente se buscan valores enteros de la variable x que satisfagan

$$ax \equiv b \pmod{m}. \tag{II - 23}$$

Estudiaremos primero un caso especial de (II - 23). La congruencia

$$ax \equiv 1 \pmod{m} \tag{II - 24}$$

es válida si y sólo si $ax = 1 + km$ o si $ax - km = 1$ para algún entero k. Entonces, según el Teorema II - 12, $ax \equiv 1 \pmod{m}$ si y sólo si $(a, m) = 1$. Por consiguiente, (II - 24) tiene una solución única si y sólo si $(a, m) = 1$. Cuando (II - 24) tiene una solución única $[b] \pmod{m}$ cualquier elemento de $[b]$ se llama *recíproco* a^{-1} de a con respecto al módulo m. En consecuencia, un entero a tiene un recíproco respecto al módulo m si y sólo si $(a, m) = 1$. Por ejemplo: 3 es recíproco de 2 con respecto al módulo 5; 4 es recíproco de 2 con respecto al módulo 7, pero 2 no tiene recíproco

con respecto al módulo 6. Siempre se puede encontrar por medio del Teorema II - 12, un recíproco de n respecto al módulo de m, en caso de que exista, dado que si $(n, m) = 1$ existen enteros A y B tales que $Am + Bn = 1$, y B es el recíproco de n con respecto al módulo m.

Consideraremos ahora la congruencia (II - 23). Si $(a, m) = 1$, entonces a tiene un recíproco a^{-1}, y podemos escribir $a^{-1}ax \equiv a^{-1}b$ (mód. m), $x \equiv a^{-1}b$ (mód. m). De esta manera (II - 23) tiene una solución si $(a, m) = 1$. En general, si $(a, m) \mid b$, se hace $(a, m) = d$; $a = a_1d$; $m = m_1d$; y $b = b_1d$. Luego $(a_1m_1) = 1$ y $a_1x \equiv b_1$ (mód. m_1) tiene una solución $x \equiv a_1^{-1}b_1$ (mód. m_1), es decir, $a_1x = b_1 + km_1$ para algún entero k. De esta ecuación obtenemos $a_1dx = b_1d + km_1d$, o $ax = b + km$, de donde (II - 23) tiene una solución si $(a, m) \mid b$. A la inversa, si $ax \equiv b$ (mód. m) tiene una solución $[r]$ (mód.m), entonces $ar = b + km$ para algún entero k, de donde $ar - km = b$ y $(a, m) \mid b$. Es así como $ax \equiv b$ (mód. m) tiene siempre solución si $(a, m) = 1$ y en general, tenemos el

TEOREMA II - 22. *La congruencia* $ax \equiv b$ (mód. m) *tiene solución si y sólo si* $d = (a, m)$ *es divisor de* b.

Por ejemplo, $2x \equiv 1$ (mód. 6) y $3x \equiv 5$ (mód. 6) no tiene soluciones; $2x \equiv 1$ (mód. 5) y $3x \equiv 9$ (mód. 6) tienen solución.

Si $ax \equiv b$ (mód. m), y $ay \equiv b$ (mód. m), entonces $ax \equiv ay$ (mód. m), y también $ax = ay + km$. Como anteriormente, sea $d = (a, m)$; $a = da_1$, $m = dm_1$. Entonces $a_1(x - y) = km_1$ y $x \equiv y$ (mód. m_1). De aquí que dos soluciones cualesquiera de (II - 23) sean congruentes con respecto al módulo m_1. *Si* $[x]$ (mód. m) es una solución de (II-23), entonces, valiéndonos de $b = db_1$, tenemos $a_1dx = b_1d + kdm_1$, de donde $a_1x = b_1 + km_1$, es decir, cualquiera solución de (II - 23) es una solución de $a_1x \equiv b_1$ (mód. m_1). Según el Teorema II - 22, $a_1x \equiv b_1$ (mód. m_1) tiene una solución $[x_0]$ (mód. m_1) que, según la demostración anterior, es única. Por consiguiente, todas las soluciones de (II - 23) pertenecen a $[x_0]$ (mód. m_1), es decir, al conjunto.

$$x_0, x_0 \pm m_1, x_0 \pm 2m_1, \ldots, x_0 \pm dm_1, \ldots$$

Dado que $x_0 + dm_1 \equiv x_0$ (mód. m), hay exactamente d soluciones (mód. m), a saber $[x_0]$, $[x_0 + m_1]$, $\ldots$, $[x_0 + (d - 1)m_1]$ (mód. m). Por eso tenemos el

TEOREMA II-23. *Si* $ax \equiv b$ (mód. m) *tiene una solución, entonces hay una solución única* (mód. m/d) *en donde* $(a, m) = d$, *y* d *soluciones* (mód. m).

Por ejemplo, $6x \equiv 9$ (mód. 15) tiene una sola solución [4] (mód. 5) y tres soluciones [4], [9], [14] (mód. 15) en donde $d = (6, 15) = 3$.

Resultados análogos al anterior pueden obtenerse para congruencias simultáneas respecto de varios módulos (ver Bibliografía Nº 43; págs. 240-249). En particular el Teorema Chino de los Restos se presta para muchos problemas interesantes. [Si los enteros $m_1, m_2, \ldots, m_t$ son primos por pares, existen enteros x para los cuales simultáneamente $x \equiv a_1$ (mód. m_1); $x \equiv a_2$ (mód. m_2), ..., $x \equiv a_t$ (mód. m_t)]. Sin embargo, en un tratado breve como el presente, deben suprimirse muchos detalles. Por este motivo, consideramos que hemos cumplido con nuestra finalidad de presentar conceptos básicos de congruencias lineales y dejamos que el lector prosiga el estudio de algunas interesantes aplicaciones, como la mencionada anteriormente, en textos dedicados enteramente a la teoría de los números.

EJERCICIOS

1. Demostrar que la factorización no es necesariamente única (mód. m) cuando m no es un número primo, mostrando dos factorizaciones distintas de $x^3 - 1$ con respecto al módulo 15.
2. Resolver las congruencias:
   a) $x^3 - 6x + 5 \equiv 0$ (mód. 4);
   b) $x^3 + 2x^2 + 4x + 3 \equiv 0$ (mód. 5).
3. ¿Cuántas soluciones tiene la congruencia $x^{17} \equiv x$ (mód. 17)?
4. Resolver la congruencia $x^7 + 2x^6 + 8x^4 + x + 3 \equiv 0$ (mód. 5).
5. Encontrar el recíproco de 7 (mód. 13), de 5 (mód. 33) y de 12 (mód. 49).
6. Resolver cuando sea posible:
   a) $4x \equiv 1$ (mód. 5);
   b) $4x \equiv 1$ (mód. 6);
   c) $6x \equiv 39$ (mód. 15);
   d) $6x \equiv 39$ (mód. 34);
   e) $1250x \equiv 1725$ (mód. 2000).
7. Encontrar todas las soluciones de las siguientes congruencias:
   a) $4x \equiv 6$ (mód. 10);
   b) $10x \equiv 8$ (mód. 16).

8. Demostrar el Teorema de Wilson: $(p-1)! \equiv -1 \pmod{p}$, para cualquier número primo p.

9. Demostrar que dos congruencias $x \equiv a \pmod{m}$ y $x \equiv b \pmod{n}$ tienen una solución común si y sólo si $a \equiv b \pmod{s}$, en donde $s = (m, n)$. (Ver Bibliografía Nº 43; págs. 241-242). Proponer un método para encontrar la solución en caso de que exista.

II-12* PROBLEMAS DIOFANTICOS. Terminaremos nuestro breve estudio de la teoría de los números, citando dos famosos problemas. El primero se refiere a las soluciones enteras de la *ecuación de Pitágoras* $a^2 + b^2 = c^2$; el segundo se conoce con el nombre de Ultimo Teorema de Fermat. Ambos problemas se refieren a soluciones enteras y pueden llamarse problemas *diofánticos*, es decir, problemas algebraicos en los que se piden soluciones racionales. Estos problemas se incluyen en la mayoría de los textos sobre teoría de los números, por ejemplo en (Bibliografía Nº 43; págs. 165-208) y (Bibliografía Nº 50; págs. 37-67 y 388-428).

La ecuación pitagórica es una expresión algebraica del *teorema de Pitágoras* que dice que en un triángulo rectángulo la suma de los cuadrados cuyos lados son iguales a los catetos es igual al cuadrado cuyo lado tiene la misma longitud que la hipotenusa. El problema de encontrar todas las soluciones enteras de la ecuación pitagórica, se convierte precisamente en el problema de encontrar todos los triángulos rectángulos cuyos lados tengan longitudes enteras. La solución particular $a = 3$, $b = 4$, $c = 5$, junto con $a = 5$, $b = 12$, $c = 13$ y con $a = 8$, $b = 15$, $c = 17$, era conocida por los escritores chinos, hindúes y egipcios de la antigüedad. Los griegos atribuyen a Pitágoras una solución algo más general

$$a = 2n + 1,\ b = 2n^2 + 2n,\ c = 2n^2 + 2n + 1, \tag{II-25}$$

donde n es cualquier entero.

Podemos verificar fácilmente, por sustitución, que (II-25) es una solución para cualquier entero n. Sin embargo, la relación $b + 1 = c$ que debe ser válida para todas las soluciones que se obtienen de (II-25), no necesita ser válida para todas las soluciones de la ecuación pitagórica. Por ejemplo, $a = 8$, $b = 15$, $c = 17$ es una solución que no se puede obtener de (II-25). Muchas otras soluciones como ésta resultan del hecho de que si a, b, c es una solu-

ción de la ecuación pitagórica, entonces da, db, dc es también una solución para cualquier entero d. De aquí que (II - 25) no proporcione todas las soluciones de la ecuación pitagórica o aún todas las soluciones tales que a, b y c sean primos entre sí, es decir, *sean soluciones primitivas*. Todas las soluciones primitivas de la ecuación pitagórica se dan en las fórmulas. (Ver Bibliogr. Nº 50; pág. 40).

(II - 26) $\quad a = r^2 - s^2,\ b = 2rs,\ c = r^2 + s^2,$

en donde $(r, s) = 1$, $0 < s < r$, $r \not\equiv s \pmod 2$.

El otro problema que mencionaremos ha sido un constante desafío para los matemáticos por más de trescientos años.

TEOREMA II - 24. ULTIMO TEOREMA DE FERMAT. *Si n es un entero mayor que 2, no existen enteros x, y, z, tales que $x^n + y^n = z^n$, siendo $xyz \neq 0$.*

Fermat concibió este teorema como una extensión de la ecuación pitagórica (ver Bibliografía Nº 43; págs. 203-207) y señaló que tenía "una demostración verdaderamente maravillosa" de él, pero nunca formuló la demostración. Aun cuando se han ofrecido importantes premios por una demostración y aunque el teorema ha sido probado para todos los $n \leq 617$, aún no se ha hallado una demostración general.

H. S. Vandiver hizo en 1946, una síntesis de todo lo relacionado con este teorema hasta esa fecha. (Ver Bibliografía Nº 51).

En todo este capítulo hemos considerado las propiedades del anillo de los enteros. La divisibilidad y el Algoritmo de la División se utilizaron en el estudio de los números primos, de la factorización única, y en el Algoritmo de Euclides. Se ha examinado también la representación de números en diversas bases. En la notación decimal se vio que todo número racional puede representarse en forma de decimal periódico y a la inversa. Se utilizó el concepto de una congruencia con respecto a un módulo entero m para verificar varios métodos corrientes de comprobar la divisibilidad y los cálculos aritméticos. También se empleó este concepto para subdividir el conjunto de enteros en clases residuales o de congruencia. El concepto de clase residual nos llevó a aquél de un sistema residual completo respecto al módulo m que comprende exactamente un

elemento de cada clase. Se descubrió en seguida que en cualquier sistema residual completo con respecto al módulo m, los elementos primos respecto de m constituían un sistema residual reducido respecto al módulo m. Dada una raíz m-ésima primitiva de la unidad, se obtuvieron todas las raíces m-ésimas por medio de cualquier sistema residual completo respecto al módulo m, y todas las m-ésimas raíces primitivas por medio de cualquier sistema residual reducido respecto al módulo m. Las propiedades de un sistema residual reducido sirvieron para demostrar dos teoremas clásicos en la teoría de los números, el Teorema de Euler y el Teorema Simple de Fermat. Finalmente, nos hemos referido de modo breve a las congruencias lineales y a los problemas diofánticos. Nuestro propósito ha sido principalmente presentar unos cuantos conceptos fundamentales y de este modo ofrecer en particular una mejor interpretación de las propiedades y comportamiento de los enteros a los lectores que no tengan la oportunidad de emprender un curso completo en este aspecto de las matemáticas. En el capítulo siguiente volveremos a considerar muchas de las propiedades del anillo de los enteros como propiedades de un anillo de polinomios.

EJERCICIOS

1. Demostrar que todas las soluciones primitivas de la ecuación pitagórica están dadas por las relaciones (11-26). (Ver Bibliografía Nº 50; págs. 38-40).

2. Hacer una lista de los veinte triángulos rectángulos que es posible obtener con los tres lados de longitudes enteras y el mayor de una longitud que no sobrepase las cincuenta unidades.

3. En una clase de 12 niños tienen b manzanas por cada niño para el almuerzo. En otra clase de 8 niños tienen c naranjas por niño. Encontrar dos pares posibles de valores de b y c, tales que los niños de las dos clases puedan hacer un intercambio de las frutas y distribuirlas equitativamente. ¿Cuáles son los valores positivos menores posibles de b y c? Proponer una solución completa del problema utilizando clases de congruencia.

4. Discutir la obra y métodos de Diofanto de Alejandría.

CAPITULO III

Teoría de los polinomios

En el Capítulo I hemos definido los números racionales, algebraicos, trascendentes y reales, valiéndonos de los números enteros positivos. En el Capítulo II se han examinado las propiedades del anillo de los enteros. En este capítulo nos serviremos de un anillo de polinomios en una variable para definir funciones racionales, algebraicas, trascendentes y analíticas. Se tratará la divisibilidad, el Algoritmo de la División, el Algoritmo de Euclides y las propiedades en el anillo de los polinomios que corresponden a los números primos, bases y congruencias en el anillo de los números. Nuestro propósito es triple: comprender las propiedades básicas de los polinomios; examinar las relaciones entre los polinomios y otras funciones ordinarias; e introducir unos cuantos conceptos que necesitaremos en el estudio de la teoría de las ecuaciones en el Capítulo IV.

III-1 POLINOMIOS. En los primeros dos capítulos nos hemos preocupado principalmente de los números: los números enteros, racionales, los números reales, los números complejos. Ahora, presentaremos un nuevo conjunto de símbolos x, y, t, ... y consideraremos la igualdad, la adición, la sustracción, la multiplicación y la división en el conjunto total compuesto de los nuevos símbolos y de los números complejos. Los nuevos símbolos pueden considerarse sencillamente como símbolos sin atribuirles conjuntos de valores o suponerles relaciones. En este caso se llaman *indeterminadas*. Los nuevos símbolos pueden ser considerados también como *variables* que adquieren valores de un subconjunto del

conjunto de los números complejos. Frecuentemente llamaremos variables a los símbolos, aun cuando mencionemos a veces propiedades correspondientes a las indeterminadas. Una gran parte de la teoría que se estudia en este capítulo se referirá a las variables e indeterminadas.

Dada cualquiera indeterminada x, definiremos el símbolo x^n en que n es cualquier entero positivo, como el producto de n factores x, $x^0 = 1$, $x^{-n}x^n = 1$, y $(x^{1/n})^n = x$. Definiciones análogas son válidas para cualquier variable x, con la excepción de que x^0 y x^{-n} son indefinidas cuando $x = 0$. La adición y la multiplicación de los nuevos símbolos y de los números complejos son, por definición, únicas, conmutativas, asociativas y satisfacen las leyes de distributividad. Por eso $ax + bx = (a + b)x$ y $(ax)(bx) = abx^2$, siendo a, b números complejos cualesquiera.

El producto de cualquier conjunto de números complejos y de los nuevos símbolos se llama *un monomio*. Por ejemplo, 15, x, $2x$, $5x^3y^4t$, y $3\sqrt{2xy}$ son monomios. La suma de dos monomios se llama *binomio*. Una suma de tres monomios se llama *trinomio* y, en general, una suma de uno o más monomios se denomina *polinomio*.

Un monomio de la forma bx^m, en donde m es un entero no negativo y b es un número complejo, se llama un monomio en x con *coeficiente* b y, cuando $b \neq 0$, de *grado* m. Cualquier número complejo b es por sí mismo un monomio. El monomio 0 no tiene grado. Cuando $b \neq 0$, el monomio $b = bx^0$ tiene grado 0.

Un polinomio de la forma

$$a_0x^m + a_1x^{m-1} + \ldots + a_{m-1}x + a_m, \tag{III - 1}$$

en donde los a_i son números complejos y $a_0 \neq 0$, se llama un polinomio de grado m en x. Los a_i se llaman los coeficientes del polinomio. El coeficiente a_0 distinto de cero con que comienza el polinomio se llama el *coeficiente inicial*. Dado que las indeterminadas *no* tienen valores numéricos, dos polinomios en una indeterminada x son iguales si y sólo si los coeficientes de las potencias correspondientes de x son iguales. Así, para una indeterminada x, la ecuación

$$ax^2 + bx + c = x + 2$$

implica que $a = 0$, $b = 1$, y $c = 2$. Dos polinomios en una variable x pueden ser iguales para cualquier número entero no negativo

de valores de la variable x. Por consiguiente, la ecuación $x^2 - 2x - 3 = 0$ implica que $x = 3$ o $x = -1$, para una variable x.

El grado de un polinomio depende de la variable que se considere. Por ejemplo, $3x^4y^6$ es de grado dos en x con coeficiente $3y^6$ y de grado cinco en y con coeficiente $3x^4$. El polinomio $10x^6$ puede ser considerado como un polinomio de grado seis en x con coeficiente 10, o como un polinomio de grado dos en $2x^3$ con coeficiente $\frac{5}{2}$, o como un polinomio de grado doce en $\sqrt{x}$ con coeficiente 10 y de muchas otras maneras más. Emplearemos la notación $p(x)$ para indicar un polinomio en x, y $p(\sqrt{2x})$ para indicar un polinomio en $\sqrt{2x}$.

EJERCICIOS

1. Haga una lista de cinco polinomios en x.
2. Indique el coeficiente inicial y el grado de cada uno de los polinomios del Ejercicio 1.
3. Hallar el coeficiente para los casos en que $36x^4$ es considerado un polinomio en:
   a) x,
   b) $2x$,
   c) x^2,
   d) $3x^2$,
   e) $\sqrt{x}$, es decir, y en que $y^4 = x$,
   (f) $\sqrt[3]{2x}$, es decir, y en que $y^3 = 2x$.
4. Indicar el grado del polinomio en cada caso del Ejercicio 3.
5. Escribir $8x^3 + 12x^2 - 10x + 7$ en forma de polinomio en (a) $2x$, y (b) $\sqrt{x}$.
6. Dados dos polinomios $p(x)$ y $q(x)$ de grados m y n respectivamente, cuyos coeficientes sean números complejos, demostrar que el producto de los dos polinomios tiene grado $m + n$.
7. Repetir el Ejercicio 6 para el producto de un número finito cualquiera de polinomios de grados m_j.

III-2 ANILLOS DE POLINOMIOS. Todo polinomio (Cap. III - 1) consiste en una variable x y un conjunto de coeficientes $a_0, a_1, \ldots, a_m$ combinados por medio de las operacionesdel anillo: adición, sustracción y multiplicación. Los polinomios en una sola variable x se suelen clasificar de acuerdo con sus coeficientes. Por eso hablaremos de polinomios en x, con coeficientes enteros, polinomios en x con coeficientes racionales, con coeficientes reales, y con coeficientes complejos. Estos conjuntos de

polinomios se llaman a veces, respectivamente, polinomios enteros, polinomios racionales, polinomios reales y polinomios complejos en x. Cada conjunto tiene a los conjuntos precedentes como subconjuntos. La suma de dos polinomios con coeficientes enteros es un polinomio con coeficientes enteros. Se pueden hacer afirmaciones análogas con respecto al producto y a la diferencia. En consecuencia, los polinomios en x con coeficientes enteros forman un anillo. En general, dado un anillo T de números, el conjunto de polinomios en x con coeficientes pertenecientes al conjunto de números T forma un *anillo de polinomios*. Este anillo de polinomios es un dominio de integridad (ver Bibliografía Nº 34, págs. 33-34), si y sólo si T es un dominio de integridad tal como se ha definido en la introducción al Capítulo II.

Cuando los coeficientes de un conjunto de polinomios pueden ser elementos cualesquiera de un campo o sistema de números (Cap. I - 14) es posible (Cap. III - 5) aplicar el Algoritmo de la División (Cap. II - 2) al anillo de polinomios. Al efecto, en este capítulo nos ocuparemos principalmente de anillos de polinomios en los cuales los coeficientes pueden ser elementos arbitrarios, de un campo tal como el sistema de los números racionales, el sistema de los números reales, o el sistema de los números complejos.

Los polinomios de diversas variables pueden definirse como formados por un conjunto finito de variables y un conjunto de coeficientes, combinados mediante un conjunto finito de operaciones de anillo. Aun cuando frecuentemente estimemos conveniente estudiar polinomios en una sola variable, muchas de nuestras aseveraciones se aplicarán igualmente a polinomios de varias variables. La excepción más importante es el Algoritmo de la División (Cap. II - 5) y sus numerosas aplicaciones. De aquí en adelante consideraremos polinomios en una sola variable con números reales cualesquiera por coeficientes, excepto cuando se especifique expresamente de otra manera.

EJERCICIOS

1. Describir cinco anillos de polinomios que sean diferentes.
2. Describir cinco dominios de integridad de polinomios que sean diferentes (Ver Ejercicio 9, Cap. II-1).
3. Describir dos anillos de polinomios que no sean dominios de integridad.

III-3 FUNCIONES RACIONALES. En el Capítulo I se fue extendiendo gradualmente el conjunto de enteros positivos hacia el conjunto de los números racionales, hacia los números reales y los números complejos. En este capítulo consideraremos ampliaciones del conjunto de los polinomios en el conjunto de las funciones racionales (que corresponden a los números racionales) y respecto de las funciones analíticas (Cap. III - 16) (que corresponden a los números reales).

Un número racional (Cap. I - 8) puede definirse como el cuociente expreso entre dos enteros a/b, en que $b \neq 0$. Una *función racional* de una indeterminada x puede definirse como el cuociente expreso de dos polinomios $f(x)/d(x)$, en que $d(x)$ no sea idéntico a 0. Análogamente, si $f(x)$ y $d(x)$ son polinomios en una variable x, entonces el cuociente expreso $f(x)/d(x)$ se llama función racional de la variable x y se define para todos los valores de x tales que $d(x) \neq 0$. Para $d(x) = 0$ es indefinida, dado que la división por cero es indefinida. Por ejemplo, $x^2 + x + 1$ es diferente de cero para todos los valores reales de x, y asimismo la función racional $(2x^2 - x + 1)/(x^2 + x + 1)$ está definida para todos los valores reales de x. La función racional $(x^2 - 1)/(x - 2)$ está definida cuando x es una indeterminada o cuando la variable x tiene un valor diferente de 2.

Se pueden expresar, además, varios de los conceptos precedentes usando la terminología del Capítulo I - 18. El anillo de los enteros I tiene al campo de los números racionales R como su campo de cuocientes. Cuando el símbolo x se adjunta al campo R se obtiene el anillo $R[x]$ de polinomios en x con coeficientes racionales. El campo de cuocientes de $R[x]$ es $R(x)$, o sea, el campo de las funciones racionales en x. En general, si T es cualquier dominio de integridad, entonces $T[x]$ es el anillo de polinomios en x con coeficientes pertenecientes a T, y $T(x)$ designa el campo de cuocientes de $T[x]$. Este concepto es importante para nosotros porque consideraremos a veces un polinomio en x y en y, tal como

$$3x^2y + 4x - y^2 + 5,$$

como un polinomio en x con coeficientes que son polinomios en y, es decir, cualquier polinomio $p(x,y)$ perteneciente a $R[x,y]$ puede considerarse como un polinomio $p(x)$ perteneciente a $T[x]$ en donde $T = R[y]$.

EJERCICIOS

Indicar en cada ejercicio los valores de la variable real x para la cual está definida* la función racional $y = f(x)/d(x)$:

1. $3x + 2y = 1$
2. $y = \dfrac{x^2 - 4x + 3}{x^2 - 3x + 2}$
3. $xy = 5$
4. $x^2 + 2xy = y - 5$
5. $y = \dfrac{x^3 + 7x^2 + 1}{x^2 - 5x + 8}$

III-4 DIVISIBILIDAD. Comenzaremos en seguida un estudio del anillo de polinomios que es muy análogo al estudio ya realizado del anillo de los enteros en el Cap. II. Se formulará nuevamente la mayoría de las definiciones y teoremas del Capítulo II, pero esta vez aplicados a los polinomios. Este desarrollo paralelo va a contribuir a darle una mayor significación al presente estudio y a la teoría de los números.

Un polinomio $d(x)$ es divisor de un polinomio $f(x)$ si y sólo si existe un polinomio $q(x)$ tal que $f(x) = d(x) \cdot q(x)$ para todos los valores de x. Por ejemplo, $x - 1$ es divisor de $x^3 - 1$; x es divisor de $2x$; $2x - 2$ es divisor de $3x^3 - 3$ en el anillo de polinomios con coeficientes racionales, pero no es divisor de $3x^3 - 3$ en el anillo de polinomios con coeficientes enteros, ya que el cuociente $q(x)$, en este caso, no tiene coeficientes enteros. La frase "para todos los valores de x" se empleará en este texto para indicar que una relación es válida para todos los valores de la variable x para los cuales las expresiones de la relación están definidas. Si el conjunto de números al cual pertenecen los coeficientes es infinito, esta frase señala también que la relación es válida para cualquiera indeterminada x (ver Bibliografía Nº 7, pág. 82). Las ecuaciones que se verifican para indeterminadas suelen llamarse *identidades*.

El Teorema II-1 puede enunciarse, ahora, para los polinomios $f(x)$, $g(x)$, $d(x)$ como sigue: Si $d(x)$ es divisor de $f(x)$ y $f(x)$ es divisor de $g(x)$, entonces $d(x)$ es divisor de $g(x)$. Si $d(x)$ es divisor de $f(x)$ y $d(x)$ es divisor de $g(x)$, entonces $d(x)$ es divisor de $f(x) + g(x)$ y de $f(x) - g(x)$. La demostración de este teorema es exactamente análoga a aquella dada para el Teorema II-1 (Ejercicio 9).

*Los ceros de un polinomio de segundo grado se tratan en el Cap. IV-5.

Si el conjunto de *coeficientes posibles* (es decir, el conjunto de números de entre los cuales se pueden elegir los coeficientes de los polinomios en consideración) forma un sistema de números o un campo, los únicos polinomios que son divisores de todos los polinomios son las constantes diferentes de cero, es decir, los polinomios de grado cero. En consecuencia, las constantes diferentes de cero son *las unidades* para el anillo de los polinomios. Sin embargo, sólo $+1$ es la unidad, o sea el elemento de identidad para la multiplicación.

En la teoría de los números (Teorema II - 8) hemos considerado a cualquier entero diferente de cero como el producto de una unidad y un entero positivo. En la teoría de los polinomios definiremos un polinomio con coeficiente inicial $+1$ como un *polinomio primitivo*. Luego, suponiendo que el conjunto de coeficientes posibles forma un sistema de números, cualquier polinomio (III - 1) excepto la constante 0, puede expresarse como el producto de una unidad y un polinomio primitivo. Por ejemplo, $2x^2 - 2 = 2(x^2 - 1)$ y $3x + 2 = 3(x + \frac{2}{3})$. El último ejemplo ilustra la necesidad de suponer que el conjunto de coeficientes posibles forma un sistema de números, de modo que sea posible la división por el coeficiente inicial del polinomio.

En la definición siguiente *del* máximo común divisor entre dos polinomios resulta evidente la correspondencia entre polinomios primitivos y los enteros positivos. Cualquier polinomio $d(x)$ que sea divisor de $f(x)$ y de $g(x)$ es divisor común de $f(x)$ y $g(x)$. Si $d(x)$ es un polinomio primitivo y todo divisor común de $f(x)$ y de $g(x)$ es también divisor de $d(x)$, entonces $d(x)$ es *el máximo común divisor* de $f(x)$ y $g(x)$. De la misma manera las definiciones de común múltiplo, mínimo común múltiplo, y primos entre sí, son exactamente análogas (Ejercicio 10) a aquellas dadas para los enteros (Cap. II - 1). En la teoría de los polinomios, $2x$ y $2x^2 - 2$ son primos entre sí, dado que su máximo común divisor es una unidad.

Dos enteros tienen el mismo valor absoluto o valor numérico si cada uno de ellos puede expresarse como el producto del otro por una unidad. Dos polinomios se llaman *asociados* si cada uno de ellos puede expresarse como el producto del otro por una unidad, es decir, $f(x)$ y $g(x)$ son asociados si $f(x)|g(x)$ y $g(x)|f(x)$. Por

ejemplo, $x - 2$, $5x - 10$, $7x - 14$, y $x/2 - 1$, son todos asociados si sus coeficientes son racionales.

Cuando el conjunto de coeficientes posibles forma un sistema de números, todo polinomio $p(x)$, excepto la constante cero, tiene un polinomio primitivo asociado único. Las unidades que se definieron anteriormente son precisamente las asociadas de la unidad. Se dice que dos polinomios que no son asociados son *independientes.*

EJERCICIOS

1. ¿Forma un anillo el conjunto de polinomios de grado par en x? ¿Forma un anillo el conjunto de polinomios en x^2? ¿Forma alguno de estos conjuntos también un dominio de integridad?
2. Escriba tres polinomios y en seguida exprese cada uno de ellos como el producto de una unidad y un polinomio primitivo.
3. ¿Puede expresarse todo polinomio de un anillo cualquiera de polinomios como el producto de una unidad y un polinomio primitivo. Dar ejemplos.
4. Repetir el Ejercicio 3 para un dominio de integridad cualquiera.
5. Repetir el Ejercicio 3 para polinomios con coeficientes pertenecientes a un campo cualquiera.
6. Proponer tres asociados de $x^3 - x^2 + 7x - 5$.
7. Proponer dos polinomios independientes que tengan un divisor común $x - 2$.
8. Proponer dos polinomios que sean asociados si el conjunto de coeficientes posibles es el conjunto de los números reales, pero que no sean asociados cuando el conjunto de coeficientes posibles es el anillo de los enteros.
9. Demostrar el Teorema II-1 para polinomios en x con coeficientes complejos.
10. Definir *común múltiplo, mínimo común múltiplo,* y *primos entre sí* para polinomios en x.

III-5 EL ALGORITMO DE LA DIVISION. En el Capítulo II-2 el Algoritmo de la División se enunció para los enteros como sigue: si a y b son dos enteros positivos cualesquiera, existen enteros q y r, $0 \leqq q$, $0 \leqq r < a$, tales que $b = qa + r$. En la teoría de los polinomios, la condición de que los enteros sean positivos puede ser reemplazada por la condición de que los polinomios sean polinomios primitivos. En este caso tendríamos: si $p(x)$ y $q(x)$ son los dos polinomios primitivos cualesquiera, existen polinomios $s(x)$ y $r(x)$ tales que $p(x) = s(x) \cdot q(x) + r(x)$ para todos los valores de x, y o bien $r(x)$ es

idéntico a cero o el grado de $r(x)$ es menor que el de $q(x)$. Por ejemplo, si $p(x) = x^4 - 5x + 6$ y $q(x) = x - 3$, entonces $s(x) = x - 2$ y $r(x) = 0$; si $p(x) = x^3 - 2x^2 + 7x - 5$ y $q(x) = x^2 - x + 1$, entonces $s(x) = x - 1$ y $r(x) = 5x - 4$. Esta forma del Algoritmo de la División puede demostrarse fácilmente, pero no es la forma más útil del teorema. Una de las desventajas es que aun cuando $r(x)$ no sea idéntico a cero, no es necesariamente un polinomio primitivo. Por ejemplo, $r(x) = 5x - 4$ en el ejemplo anterior.

Es costumbre reemplazar la condición de que los polimonios $p(x)$ y $q(x)$ sean polinomios primitivos por una suposición, como en la discusión de los polinomios primitivos (Cap. III - 4): la suposición de que el conjunto de coeficientes posibles formen un campo tal como el sistema de números racionales, reales o complejos. Según esta suposición, el Algoritmo de la División puede enunciarse como sigue para polinomios en una variable:

TEOREMA III - 1. *Si $p(x)$ y $q(x)$ son dos polinomios cualesquiera con coeficientes pertenecientes a un campo, existen entonces polinomios $s(x)$ y $r(x)$ tales que $p(x) = s(x) \cdot q(x) + r(x)$ para todos los valores de x, y o bien $r(x)$ es idéntico a cero o el grado de $r(x)$ es menor que el de $q(x)$.*

La demostración del Teorema III - 1 corresponde en principio a la "demostración" sucinta del Algoritmo de la División del Capítulo II - 2, dado que ahora se han determinado las propiedades de nuestro sistema de números. Los pormenores de la demostración se dejan como ejercicio para el lector. La necesidad de suponer que el conjunto de coeficientes posibles forma un campo es evidente, como se muestra en el ejemplo siguiente: si $p(x) = x^6 - 2x^5 + 3x^3 + 1$ y $q(x) = 2x^3 + 3x + 1$, entonces tenemos

$$x^6 - 2x^5 + 3x^2 + 1 =$$

$$\left(\frac{x^4}{2} - \frac{7}{4}x^3 + \frac{19}{8}x^2 - \frac{43}{16}x + \frac{139}{32}\right)(2x^2 + 3x + 1) + \left(-\frac{331}{32}x - \frac{107}{32}\right),$$

en donde $$s(x) = \frac{x^4}{2} - \frac{7}{4}x^3 + \frac{19}{8}x^2 - \frac{43}{16}x + \frac{139}{32}$$

y $$r(x) = -\frac{331}{32}x - \frac{107}{32}.$$

De este modo el Teorema II-1 comprende sólo las operaciones del anillo para x, pero las cuatro operaciones racionales para los coeficientes.

Puede verificarse fácilmente que el Algoritmo de la División no se pueda hacer extensivo inmediatamente a polinomios de dos o más variables. Dados dos polinomios $p(x,y)$ y $q(x,y)$, buscaremos polinomios $s(x,y)$ y $r(x,y)$ tales que

$$p(x,y) \equiv q(x,y) \cdot s(x,y) + r(x,y) \qquad \text{(III - 2)}$$

para todos los valores de x e y, y tales que $r(x,y)$ sea o bien idéntico a cero o tenga un grado menor que $q(x,y)$. En particular, para $p(x,y) \equiv x$, y para $q(x,y) \equiv y$, buscaremos polinomios $s(x,y)$ y $r(x,y)$ tales que

$$x \equiv y \cdot s(x,y) + r(x,y) \qquad \text{(III - 3)}$$

para todos los valores de x e y, es decir, tales que (III - 3) sea una identidad (Cap. III - 4). Ya que $q(x,y) \equiv y$ tiene grado uno, $r(x,y)$ debe ser una constante. Dado que el grado del miembro de la derecha de la identidad (III - 3) no puede exceder el grado del miembro de la izquierda, $s(x,y)$ debe ser también una constante. Asimismo buscaremos constantes m y b tales que $x \equiv my + b$ para todos los valores de x e y. Puesto que (Cap. II - 1) no existen constantes m y b que satisfagan estas condiciones, no es posible encontrar polinomios $s(x,y)$ y $r(x,y)$ que satisfagan la identidad (III - 3). De este modo, excepto para casos especiales, no es posible encontrar polinomios $s(x,y)$ y $r(x,y)$ que satisfagan (III - 2). Por lo tanto, el Teorema III - 1 debe alterarse antes de que pueda aplicarse a polinomios de dos o más variables. Por ejemplo (III-3) puede escribirse en la forma $x \equiv 1 \cdot y + (x - y)$, en donde $r(x,y) \equiv x - y$ tiene el mismo grado que $y \equiv q(x,y)$. En el Capítulo III - 7 se considera una modificación más útil de este teorema.

Lo mismo que en la teoría de los números, el Algoritmo de la División para polinomios sirve como base para el Algoritmo de Euclides para polinomios (Cap. III - 7). En vista de las dificultades experimentadas con polinomios de dos variables, es de esperar que sea necesaria alguna modificación del Algoritmo de Euclides cuando se consideren polinomios de dos o más variables.

Aplicaremos el Algoritmo de la División a polinomios en una variable al calcular el máximo común divisor de dos polinomios

(Cap. III - 7); al expresar un polinomio $p(x)$ en la forma $q(bx + d)$ (Cap. III - 8); al determinar el número exacto de raíces reales distintas de una ecuación polinomia con coeficientes reales (Cap. IV - 12) y al determinar las raíces múltiples de una ecuación polinomia con coeficientes complejos (reales o imaginarios) (Cap. IV - 13).

EJERCICIOS

Determinar $s(x)$ y $r(x)$ según el Teorema III-1 para cada uno de los siguientes pares de polinomios.

1. $p(x) = x^2 - 3x + 4$, $q(x) = x - 2$.
2. $p(x) = 2x^2 - 3x + 4$, $q(x) = 3x - 2$.
3. $p(x) = x^3 - 5x^2 + 7x + 11$, $q(x) = x^2 + x - 1$.
4. $p(x) = x^4 + 3x^3 - 2x^2 + 2x - 1$, $q(x) = 3x^2 - 2x + 5$.
5. $p(x) = (1 - \sqrt{2})x^3 + (1 + \sqrt{2})x^2 + \sqrt{2}$, $q(x) = (1 + \sqrt{2})x^2 + (2 - \sqrt{2})$.

III-6 POLINOMIOS IRREDUCIBLES.

En el Cap. II - 3 se clasificaron los enteros de acuerdo con los enteros de los cuales eran divisores, o de acuerdo con los enteros por los cuales eran divisibles. Se encontró que todos los enteros pertenecen a una de las cuatro clases: cero, unidades, números primos y números compuestos. Análogamente encontraremos que todos los polinomios pertenecen a una de las cuatro clases: cero, unidades, polinomios irreducibles y polinomios reducibles.

Las unidades son divisores de todo polinomio y, cuando el conjunto de los coeficientes posibles forma un campo, se componen de las constantes diferentes de cero (Cap. III - 4). Se dice que un polinomio es *irreducible* si no es igual a cero ni a una unidad y si sus únicos divisores son sus asociados y las unidades. Un polinomio se llama *reducible* si tiene dos o más divisores irreducibles (no necesariamente distintos). Todos los polinomios lineales son irreducibles. La irreducibilidad de los polinomios de grado mayor que uno suele depender del conjunto de coeficientes posibles (Cap. III - 4). Por ejemplo, $x^2 - 2$ es irreducible en el anillo de polinomios con coeficientes racionales, y es reducible en el anillo de polinomios con coeficientes reales.

En la teoría de los números fue conveniente suponer que los números primos negativos estaban expresados como un producto

de una unidad y un número primo positivo. En la teoría de los polinomios a menudo será conveniente suponer que todo polinomio irreducible está expresado como el producto de una unidad y de un polinomio primitivo irreducible (Cap. III - 4).

Vamos a utilizar las definiciones precedentes y a resumir algunas de las correspondencias entre los elementos y propiedades de la teoría de los números y la teoría de los polinomios. Si el conjunto de coeficientes posibles forma un campo, los enteros m con elemento de identidad para la adición, cero, y unidades $+ 1$ y $- 1$ corresponden a los polinomios $p(x)$ con elemento de identidad para la adición, cero y unidades b, en que b es cualquier elemento diferente de cero en el conjunto de coeficientes posibles. Cualquier entero diferente de cero puede expresarse como el producto de una unidad y un entero positivo; cualquier polinomio que no es idéntico a cero puede expresarse como el producto de una unidad y un polinomio primitivo. Los enteros primos y compuestos corresponden respectivamente a los polinomios irreducibles y reducibles. El valor absoluto de un entero corresponde al grado de un polinomio. Por ejemplo, un entero m con $|m| = 0$ o un polinomio $p(x)$ sin grado es idéntico a cero; un entero m con $|m| = 1$ o un polinomio con grado cero es una unidad; un entero m con $|m| > 1$ o un polinomio con grado positivo no es ni cero ni una unidad. En el siguiente esquema se muestra la mayoría de las correspondencias básicas entre el anillo de los enteros m y el anillo de los polinomios $p(x)$:

enteros m	polinomios $p(x)$
cero	cero
unidad, $+ 1$	unidad, $+ 1$
unidades, $+ 1$ y $- 1$	constantes diferentes de cero
enteros positivos	polinomios primitivos
enteros primos	polinomios irreducibles
enteros compuestos	polinomios reducibles
valor absoluto de m	grado de $p(x)$
$\|m\| > 1$	grado positivo de $p(x)$

Estas correspondencias serán útiles al formular respecto de los polinomios algunos de los teoremas de la teoría de los números. Por ejemplo, el Teorema II - 2 puede enunciarse de la siguiente manera para los polinomios:

TEOREMA III - 2. *Todo polinomio de grado positivo tiene un polinomio primitivo divisor irreducible.*

La demostración de este teorema puede obtenerse de aquélla del Teorema II - 2 valiéndose de las analogías señaladas. Sea dado el polinomio $p(x)$ de grado m. Si $p(x)$ es irreducible, su polinomio primitivo asociado es su polinomio primitivo divisor irreducible. Si $p(x)$ es irreducible, entonces $p(x) = p_1(x) \cdot p_2(x)$, en que los $p_j(x)$ tienen grado m_j positivo, siendo $j = 1, 2$ y $m_1 + m_2 = m$. Si ningún $p_j(x)$ es irreducible, entonces $p(x) = p_{11}(x) \cdot p_{12}(x) \cdot p_{21}(x) \cdot p_{22}(x)$, en donde ningún p_{jk} es una unidad, es decir, $0 < m_{jk}$. Este proceso debe concluir después de un número finito de etapas, ya que la suma de los enteros positivos m_{jk} es un entero m positivo dado (Ejercicio 7, Cap. III - 1). Por eso $p(x)$ tiene a lo sumo m divisores y debe tener un divisor que sea un polinomio irreducible. Si el conjunto de coeficientes posibles forma un campo, todo polinomio diferente de cero tiene entre sus asociados un polinomio primitivo. Luego, todo polinomio $p(x)$ de grado no negativo tiene un divisor que es un polinomio irreducible primitivo.

En el Ejercicio 1 se enuncia el Teorema II - 3 con respecto a los polinomios. El Teorema II - 4 no se puede hacer extensivo de inmediato a la teoría de los polinomios. Por ejemplo, en el anillo de los polinomios con coeficientes reales, el conjunto de polinomios irreducibles tiene un subconjunto infinito no numerable, ya que $x - b$ es irreducible para todo número real b. La mayoría de los otros teoremas de las Secciones 3 y 4 del Capítulo II se formulan con respecto a los polinomios en los ejercicios siguientes. Las demostraciones pueden obtenerse de las correspondientes del Capítulo II, aprovechando las analogías ya citadas.

Muchos de los ejercicios siguientes y sus demostraciones pueden enunciarse con respecto a polinomios de varias variables. Por ejemplo (Ejercicio 9), el Teorema II - 8 de Factorización Unica, es válido para polinomios de cualquier número finito de variables con coeficientes enteros, racionales, reales o complejos (Ver Bibliografía Nº 7; págs. 97-100).

EJERCICIOS

1. Demostrar que cualquier polinomio reducible $p(x)$ de grado m tiene un divisor polinomio primitivo irreducible de grado $\leq m/2$.

2. Proponer ejemplos para el Ejercicio 1 cuando $m = 2, 3, 5$ y 7.

3. Demostrar que si $p(x)$ es un polinomio irreducible y $q(x)$ es cualquier polinomio, entonces o bien $p(x)$ es divisor de $q(x)$ o ambos polinomios son primos entre sí.

4. Proponer ejemplos que ilustren los dos casos del Ejercicio 3.

5. Si $r(x)$ y $s(x)$ son dos polinomios cada uno de grado menor que m, y $p(x)$ es un polinomio irreducible de grado m, demostrar que $p(x)$ no es divisor de $r(x) \cdot s(x)$.

6. Dar dos ejemplos que ilustren el Ejercicio 5.

7. Si un polinomio irreducible $p(x)$ es divisor del producto

$$q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_n(x),$$

demostrar que $p(x)$ es divisor de por lo menos uno de los polinomios $q_1(x)$, $q_2(x)$, $\ldots$, $q_n(x)$, en donde n es cualquier entero positivo.

8. Proponer dos ejemplos que ilustren el Ejercicio 7.

9. Demostrar que, excepto por el orden de los factores, todo polinomio que no es idéntico a cero puede representarse de una y sólo una manera como un producto de una unidad y un número finito de polinomios primitivos irreducibles.

10. Demostrar que el número de divisores independientes de

$$p(x) = c[r_1(x)]^{a_1} \cdot [r_2(x)]^{a_2} \cdot \ldots \cdot [r_k(x)]^{a_k}$$

es $(a_1 + 1)\ (a_2 + 1) \ldots (a_k + 1)$, en donde los $r_j(x)$ son polinomios distintos irreducibles, c es una constante y las a_j son enteros positivos.

11. Proponer un ejemplo que ilustre el Ejercicio 10, para el caso de $k = 3$, y enumerar los divisores independientes.

12. Repetir el Ejercicio 11 para $c \neq 1$ y $k > 3$.

13. Si $r(x)$ es el máximo común divisor y $s(x)$ es el mínimo común múltiplo de dos polinomios primitivos $p(x)$ y $q(x)$, demostrar que $r(x) \cdot s(x) = p(x) \cdot q(x)$.

14. Formular el Postulado de Arquímedes con respecto a los polinomios (Cap. II-2) y proponer un ejemplo.

15. Formular con respecto a los polinomios cada una de las tres partes del Teorema II-9.

16. Dar ejemplos que ilustren cada uno de los enunciados del Ejercicio 15.

III-7 EL ALGORITMO DE EUCLIDES.

El Algoritmo de Euclides se usó en el Cap. II-5 con el objeto de encontrar el máximo común divisor entre dos enteros sin tener que expresar ninguno de los dos enteros en sus factores primos. Emplearemos el mismo procedimiento para los polinomios $p(x)$ con el objeto de encontrar el máximo común divisor de dos polinomios sin tener que expresar ninguno de los dos polinomios en

función de sus factores irreducibles. El Teorema II - 11 puede enunciarse de la siguiente manera para los polinomios:

TEOREMA III - 3. *El máximo común divisor $r_n(x)$ de dos polinomios cualesquiera $f_0(x)$ y $f_1(x)$ de grado positivo con coeficientes pertenecientes a un campo, puede encontrarse por medio del Algoritmo de Euclides, pues es el último resto polinómico que no es igual a cero. Existen polinomios $A(x)$ y $B(x)$ tales que $r_n(x) = A(x) \cdot f_0(x) + B(x) \cdot f_1(x)$ para todos los valores de x.*

Podemos demostrar la primera parte del teorema aplicando reiteradamente el Algoritmo de la División (Cap. III - 5). El procedimiento para los polinomios $f_0(x)$ y $f_1(x)$ se ilustra en el siguiente esquema, en donde b es una constante diferente de cero que hay que determinar, el grado de $r_1(x)$ es menor que el de $f_1(x)$ y el grado de $r_j(x)$ es menor que el de $r_{j-1}(x)$ para $j = 2, 3, \ldots, n$.

$$
\begin{aligned}
f_0(x) &= q_1(x)f_1(x) + r_1(x),\\
f_1(x) &= q_2(x)r_2(x) + r_2(x),\\
r_1(x) &= q_3(x)r_3(x) + r_3(x),\\
&\cdot\\
&\cdot\\
&\cdot\\
r_{n-2}(x) &= q_n(x)r_{n-1}(x) + br_n(x),\\
r_{n-1}(x) &= q_{n+1}(x)r_n(x).
\end{aligned}
$$

En este esquema es conveniente suponer que el coeficiente inicial (Cap. III - 1) de $r_n(x)$ se ha hecho igual a + 1 dividiendo ambos miembros de la penúltima ecuación por una constante adecuada b. Luego $r_n(x)$ es un polinomio primitivo y siguiendo el mismo razonamiento que en el Cap. II - 5, es el máximo común divisor de $f_0(x)$ y $f_1(x)$. Si se conviene en que $r_n(x)$ sea un polinomio primitivo, los factores constantes (unidades) pueden insertarse o eliminarse de cualquiera ecuación del esquema. Esto significa principalmente que cualquier resto polinómico puede reemplazarse por cualquiera de sus asociados en cualquier momento.

La demostración de la existencia de polinomios $A(x)$ y $B(x)$ en la segunda parte del teorema es también análoga a aquélla del Cap. II - 5. Expresaremos sucesivamente $r_2(x)$, $r_3(x)$, ..., $r_n(x)$ en la forma $r_j(x) = A_j(x)f_0(x) + B_j(x)f_1(x)$. Todos los pormenores de la prueba se dejan al lector como ejercicio.

El Algoritmo de Euclides, tal como el Algoritmo de la División en el cual se fundamenta, no se puede hacer extensivo directamente a polinomios de dos o más incógnitas. Por ejemplo, aún cuando el máximo común divisor de x e y es 1, no existe una ecuación de la forma $Ax + By = 1$, en donde A y B sean constantes, que sea válida para todos los valores de x y de y. Es posible una extensión del teorema si se considera $f_0(x_1, x_2, \ldots, x_n)$ y $f_1(x_1, x_2, \ldots, x_n)$ como polinomios en x_n con polinomios como coeficientes de las primeras $n - 1$ variables. Entonces las A y B son funciones racionales de las primeras $n - 1$ variables, dado que se han aplicado a los coeficientes de la División Algorítmica, las cuatro operaciones racionales. (Cap. III - 5). Por ejemplo, si se considera los polinomios x e y como polinomios en y con coeficientes en x, tenemos $(1/x) \cdot x + 0 \cdot y = 1$.

Ordenaciones análogas a las que se usaron en el Cap. II - 5 para encontrar n_k, A, B, pueden emplearse también para polimonios en una variable. En general, tenemos

$$\begin{array}{c} f_0 \; f_1 \; r_1 \; r_2 \; \ldots \; r_n \; 0 \\ q_1 \; q_2 \; q_3 \; \ldots \; q_{n+1} \end{array}$$

Dado que el cálculo de los q y r exige corrientemente cálculos escritos, cambiaremos entre sí el orden de las dos filas y usaremos la ordenación

$$\begin{array}{c} q_1 \; q_2 \; q_3 \; \ldots \; q_{n+1} \\ f_0 \; f_1 \; r_1 \; r_2 \; \ldots \; r_n \; 0 \\ q_1 f_1 \; q_2 r_1 \; q_3 r_2 \; \ldots \\ a_1 r_1 \; a_2 r_2 \; a_3 r_3 \; \ldots \end{array}$$

en donde $a_1 r_1 = f_0 - q_2 f_1$, $a_2 r_2 = f_1 - q_3 r_1$, ..., y los a_j son constantes arbitrarias.

Si $f_0(x) = x^4 - 3x^3 + 2x$ y $f_1(x) = x^3 - x$, tenemos el esquema

$$\begin{array}{lll} & x - 3 & x + 1 \\ x^4 - 3x^3 + 2x & x^3 - x & x^2 - x \quad 0 \\ \underline{x^4 - x^2} & \underline{x^3 - x^2} & \\ -3x^3 + x^2 + 2x & x^2 - x & \\ \underline{-3x^3 + 3x} & \underline{x^2 - x} & \\ x^2 - x & 0 & \end{array}$$

de donde el máximo común divisor es $x^2 - x$. Este esquema se puede ampliar para que resulte $A(x)$ y $B(x)$, como el Cap. II-5. Los

detalles algebraicos para el cálculo de $r_n(x)$ suelen simplificarse en forma notable por medio de la multiplicación cruzada. (Ver Bibliografía Nº 37).

De la misma manera que para los números, el máximo común divisor puede obtenerse observando si ambos polinomios están expresados en sus factores irreducibles (Ejercicio 9, Cap. III-6). El Algoritmo de Euclides proporciona un procedimiento para determinar el máximo común divisor de dos polinomios sin necesidad de factorizar los polinomios. Este algoritmo tiene también aplicaciones importantes y muy prácticas en la determinación del número de raíces de una ecuación polinomia (Secciones 12 y 13 del Cap. IV).

En la sección siguiente de este Capítulo, continuaremos nuestro desarrollo de la teoría de los polinomios y buscaremos un concepto que corresponda al concepto de base (Cap. II - 6) en la teoría de los números.

EJERCICIOS

Por medio del Algoritmo de Euclides, encontrar el máximo común divisor de cada uno de los siguientes pares de polinomios:

1. $x^4 - 5x + 6$ y $x^2 - 4$.
2. $x^6 - 3x^5 + 3x - 1$ y $x^5 - 2x + 1$.
3. $x^3 + 2x + 20$ y $3x^2 + 2$.
4. $x^4 - 6x^3 + 7x^2 + 6x - 2$ y $2x^4 - 9x^3 + 7x + 3$.

III-8 CAMBIO DE VARIABLE. Cualquier entero positivo m puede expresarse como polinomio en n, en que $n > 1$ es un entero positivo arbitrario con coeficientes pertenecientes al conjunto de los enteros $0, 1, 2, \ldots, n-1$ (Teorema II-13). Es posible enunciar este teorema de varias maneras con respecto a los polinomios. El siguiente es uno de los enunciados más útiles.

TEOREMA III - 4. *Cualquier polinomio $p(x)$ con coeficientes pertenecientes a un campo puede expresarse como polinomio respecto de un polinomio arbitrario lineal $bx + d$.*

Dado un polinomio $p(x) = x^3 - 6x^2 + 2$, podemos designar sus ceros como, r, s, t y buscar un nuevo polinomio cúbico $q(y)$ con

ceros $r - 2$, $s - 2$, $t - 2$. Este procedimiento de reducir los ceros de un polinomio se usa frecuentemente al resolver ecuaciones cúbicas (Cap. IV-9). Los métodos para obtener los nuevos polinomios se estudiarán en los Capítulos III-5 y IV-3. En el caso anterior, se encontraría que $q(y) = y^3 - 12y - 14$ o $q(x - 2) = (x - 2)^3 - 12(x - 2) - 14$, en que $x - 2 = y$. El Teorema III-4 establece que para números cualesquiera $b \neq 0$ y d pertenecientes al conjunto de los coeficientes posibles, cualquier polinomio $p(x)$ puede escribirse en la forma $q(bx + d)$.

La demostración siguiente del Teorema III-4 corresponde estrictamente a aquella del Teorema II-13. Dado un polinomio $p(x)$ de grado m y un polinomio lineal $bx + d$, aplicamos el Teorema III-1 para obtener

$$p(x) = p_1(x) \cdot (bx + d) + r_1,$$

en donde r_1 es una constante dado que, si es diferente de cero, su grado debe ser menor que el de $bx + d$. Además, el grado de $p_1(x)$ es uno menor que el de $p(x)$. Si $p_1(x)$ tiene grado positivo, podemos repetir el procedimiento. En general, ya que $p(x)$ tiene grado m, repetiremos el procedimiento m veces y obtendremos una sucesión

$$\begin{aligned}
p(x) &= p_1(x)(bx + d) + r_1,\\
p_1(x) &= p_2(x)(bx + d) + r_2,\\
&\cdot\\
&\cdot\\
&\cdot\\
p_{m-2}(x) &= p_{m-1}(x)\,(bx + d) + r_{m-1},\\
p_{m-1}(x) &= p_m(x)\,(bx + d) + r_m,
\end{aligned}$$

en que los p_j son polinomios de grado $m - j$ y los r son constantes. Designemos la constante $p_m(x)$ por r_{m+1}. Las ecuaciones precedentes pueden usarse exactamente como en el Capítulo II-6 para obtener $p(x) = r_{m+1}(bx + d)^m + r_m(bx + d)^{m-1} + \ldots + r_2(bx + d) + r_1 = q(bx + d)$.

La división sintética (Cap. IV-2) y el Teorema de Taylor (Cap. III-15) son muy útiles para efectuar los cálculos que se necesitan frecuentemente para aplicar el Teorema III-4. En consecuencia, no consideraremos aplicaciones detalladas del Teorema III-4 hasta después de que se introduzcan estos conceptos.

La mayoría de los temas restantes que hemos considerado en la teoría de los números (congruencias, clases residuales, función ϕ, problemas diofánticos), tienen una o más interpretaciones en la teoría de los polinomios. Sin embargo, dado que no necesitaremos estas interpretaciones en nuestro estudio de la teoría de las ecuaciones, mencionaremos solamente el concepto de un ideal que corresponde a una congruencia (Cap. III-9). Luego, encaminaremos nuestro estudio de la teoría de los polinomios en una nueva dirección: en las primeras ocho partes de este capítulo hemos expuesto correspondencias entre el anillo de los enteros y el anillo de los polinomios; en el Cap. III-10 iniciaremos la explicación de varios tipos de funciones del anillo de los polinomios que corresponden al estudio del Capítulo I, sobre varios sistemas de números pertenecientes al anillo de los enteros. Los ceros de los polinomios se estudiarán en el Capítulo IV.

EJERCICIOS

1. Escribir $p(x) = x^3 + 3x - 1$ como $q(x + 2)$.
2. Escribir $p(x) = x^4 + 3x^3 + 5$ como $q(x + 1)$.
3. Escribir $p(x) = x^4 + 8x^3 - 7x + 11$ como $q(x - 2)$.

*III-9 IDEALES. Concluiremos nuestro estudio de las correspondencias entre la teoría de los polinomios y la teoría de los números expuesta en el Capítulo II, refiriéndonos brevemente a un concepto relativo a las congruencias (Cap. II-8).

Dos enteros a y b son congruentes respecto de un módulo entero m si su diferencia es divisible por m. Dos polinomios $p(x)$ y $q(x)$ son congruentes módulo un polinomio $m(x)$ si su diferencia es divisible por $m(x)$. El conjunto de todos los enteros múltiplos de un entero m forma una clase residual [0] (mód. m) y constituye el *ideal* de m dentro del anillo de los enteros. El conjunto de todos los polinomios múltiplos de $m(x)$ constituye el ideal de $m(x)$ dentro del anillo de los polinomios. Por ejemplo, $x^4 + 2x$, x^5, $x^m - 12x^4$, pertenecen todos al ideal de x, mientras que $x^4 + b$ con $b \neq 0$ no pertenece al ideal de x.

Las clases residuales pueden definirse en función del ideal de $m(x)$. Sin embargo, el número de las clases residuales ya no es finito. Por ejemplo, en el anillo de los polinomios con coeficientes

enteros, cada entero representa una clase residual distinta respecto del ideal de x. Los teoremas análogos a la mayoría de los teoremas sobre residuos de la teoría de los números, cuando los hay, se encuentran fuera del alcance de nuestro breve estudio. En la Bibliografía Nº 34 se puede consultar una excelente introducción al estudio de esta materia.

EJERCICIOS

1. Describir el ideal de las siguientes expresiones en el anillo de los polinomios con coeficientes enteros:
(a) x; (b) x^2; (c) $x + 1$.

2. Un subconjunto S de uno o más elementos de un anillo R es un ideal si (i) la diferencia de dos elementos cualesquiera de S es un elemento de S; y (ii) el producto de cualquier elemento de S por un elemento de R es un elemento de S. Esta es la definición corriente de un ideal. Probar que todos los ideales del Ejercicio 1 satisfacen esta definición.

3. Valiéndose de la definición del Ejercicio 2, demostrar que cualquier ideal S perteneciente a un anillo R, debe ser también un subanillo de R.

4. Indicar cuáles de los siguientes son ideales: (a) el anillo de los enteros pares respecto del anillo de los enteros; (b) el anillo de los enteros respecto del anillo de los números racionales.

5. Un anillo S perteneciente a un anillo R se llama *ideal principal* si todo elemento de S es de la forma rb, en que b es un elemento constante y r es un elemento arbitrario de R. Cada uno de los ideales del Ejercicio 1 es un ideal principal; en realidad, siempre que el Algoritmo de Euclides se verifica en un anillo, todo ideal de ese anillo es un ideal principal. Proponer un ejemplo de un ideal que no sea un ideal principal.

III-10 FUNCIONES. Dado cualquier polinomio $p(x)$, podemos asociar un número único $p(b)$ a cada valor numérico de b asignado a x. En este caso, los valores numéricos supuestos para el polinomio $p(x)$ dependen del conjunto de valores S supuestos para la variable x. La siguiente definición de función se basa sobre esta noción de dependencia.

Se dice que la variable y es una *función* de la variable x respecto de un conjunto de números S, si a cada valor de x en S, le corresponde uno o más valores de y. La variable x se llama *variable independiente*; y, la *variable dependiente*. En rigor, la función es la regla o ley mediante la cual los valores de x dan origen a los valores de $f(x)$. Esta función o regla puede expresarse como un po-

linomio en x, como un gráfico en el plano xy y de muchas otras maneras. La relación funcional entre x e y se señala por medio de los símbolos $y = f(x)$. El conjunto de los valores de S se llama el dominio de definición, o simplemente, *el dominio* de f. El conjunto de valores que se atribuyen a y se llama rango de valores o *rango* de f. Si a cada valor de x en S, corresponde exactamente un valor de y, se dice que la función de x respecto de S es una *función uniforme*. Si para cada valor de x corresponden dos o más valores de y, se llama una *función multiforme* de x.

Teniendo en cuenta estas definiciones, las proposiciones formuladas al comienzo de esta sección (Cap. III-10) implican que cualquier polinomio $p(x)$ es una función uniforme de la variable x. Esta aseveración es una consecuencia de las definiciones del Capítulo I, ya que para cualquier valor numérico dado de x, por ejemplo b, $p(b)$ supone sólo un número finito de las operaciones de adición, sustracción y multiplicación de números. Cada una de estas operaciones ha sido definida como única. Consideremos, por ejemplo, $p(x) = x^4 - 7x^2 + 3x + 2$ para $x = 5$, en donde

$$p(5) = 5 \cdot 5 \cdot 5 - 7 \cdot 5 \cdot 5 + 3 \cdot 5 + 2$$

está unívocamente definida.

Hemos visto que el conjunto de valores, o rango de la función, depende del conjunto S de valores que se atribuye a la variable x, es decir, del dominio de la función. Es conveniente identificar los conjuntos S a los cuales se restringe x comúnmente. El conjunto de valores S suele consistir en uno o más intervalos, en donde el conjunto de todos los números reales que satisfacen cualquiera de las siguientes relaciones, se denomina un *intervalo:* $x < a$, $x \leqq a$, $a < x < b$, $a \leqq x < b$, $a \leqq x \leqq b$, $a < x \leqq b$, $b \leqq x$, $b < x$ para números reales cualesquiera a, b. El conjunto $a < x < b$ también se llama un *segmento o intervalo abierto;* $a \leqq x < b$ no es ni abierto ni cerrado y suele denominarse *intervalo semicerrado;* $a \leqq x \leqq b$ se llama *intervalo cerrado.* Cuando el conjunto S comprende a todos los números reales o a un solo intervalo de números reales tales que $x < 0$, $0 < x < 1$, ó $2 \leqq x$, x se llama *una variable real continua.* Cuando el conjunto S comprende a todos los enteros positivos, x se llama una *variable entera positiva.*

En seguida, nos prepararemos para definir una función continua (Cap. III-12). Esta preparación es uno de los propósitos prin-

cipales de esta sección y de la siguiente (Cap. III-11). La continuidad es una propiedad importante de todos los polinomios en variables continuas. En realidad, encontraremos (Ejercicio 4, Cap. III-13) que cuando x es una variable real continua, el polinomio $p(x)$ es una función continua de x. Esta propiedad de los polinomios es fundamental y se aprovecha para encontrar raíces de cualquier polinomio $p(x)$. (Ejercicio 5, Cap. III-13; Cap. IV-5). Una de las mejores definiciones de una función continua supone el concepto de límite.

El concepto de límite se considera frecuentemente como materia del análisis, tomando en cuenta que las tres principales subdivisiones de las matemáticas son álgebra, geometría y análisis. Sin embargo, los conceptos fundamentales del álgebra no pueden constituir un compartimento, una entidad estrechamente entrabada, separada totalmente de la geometría y del análisis. Un postulado sobre la existencia de todos los números reales puede usarse también para postular la continuidad de una recta en geometría (Cap. I-12). Nos hemos valido de representaciones geométricas de relaciones algebraicas para aclarar conceptos (Cap. I-12 y también Cap. I-16). De la misma manera, consideraremos, en seguida, unos cuantos temas del análisis [límite (Cap. III-11); continuidad (Cap. III-12 y 13), y derivada (Cap. III-14)] que nos servirán en nuestro estudio de la teoría de las ecuaciones (Cap. IV) y en este capítulo en la exposición de las siguientes correspondencias entre los números y las funciones:

enteros	polinomios
números racionales	funciones racionales
números algebraicos	funciones algebraicas
números trascendentes	funciones trascendentes
números reales	funciones analíticas

EJERCICIOS

1. Señalar cuáles de las funciones siguientes son funciones uniformes de x (considerar solamente los valores reales de x y de y):

(a) $y = x^3 - 3x + 1$
(b) $y = \sqrt{x^2 - 9}$
(c) $y = (x^2 - 9)^2$
(d) $y = \dfrac{x^2 + 1}{x^2 - 1}$
* (e) $y = 2^x$
* (f) $y = \log x$
* (g) $y = \operatorname{sen} x$
* (h) $y = \operatorname{arc\,sen} x$

2. Señalar el dominio de definición y el rango de valores para cada una de las funciones del Ejercicio 1.

3. Proponer cinco funciones multiformes de x.

4. Dar tres ejemplos de cada uno de los siguientes tipos de intervalos: (a) abierto; (b) cerrado; (c) ni abierto ni cerrado.

5. Indicar cuales de las siguientes definen funciones de la variable real x:

a) $y = x^2 - 3x + 1$;
b) $y = x$ para $x > 0$, $y = -x$ para $x \leqq 0$;
c) $y = x - [x]$, en que $[x]$ indica el mayor entero $\leqq x$;
d) $y = x/(x^2 - 2)$;
e) $y = 1$ si x es racional, $y = 0$ si x es irracional;
*f) $y = \tan x$;
g) $y = 2$ para $x < -1$; $y = -x$ para $-1 \leqq x \leqq 0$, $y = 1/x$ para $0 < x$.

6. Repetir el Ejercicio 5 para el caso en que el dominio de definición de x es el conjunto de (a) los números racionales; (b) los enteros positivos.

7. Si $f(y)$ está dado por $x = y^n$, entonces el valor principal de la función inversa $f^{-1}(x)$ está dado por $y = x^{1/n}$. Aprovéchese esta relación para definir $x^{1/n}$ para (i) $x > 0$ y cualquier entero $n \neq 0$; y (ii) cualquier valor real de x y cualquier entero impar n (Ejercicio 13 Cap. 1 — 12). Determinar las funciones inversas de cada una de las siguientes:

a) $x = y + 2$
b) $x = 2y$
c) $x = 3y + 5$
d) $x = y^3$
e) $x = y^{2/3}$
f) $x = (y + 1)/(y - 1)$
g) $x = (ay + b)/(cy + d)$, en donde $ad - bc \neq 0$ (Ver Teorema IV — 8)
h) $y = g(x)$
*i) $x = \operatorname{sen} y$
*j) $x = 2^y$
*k) $x = \log_3 y$.

8. Discutir las relaciones entre los dominios y rangos de $f(y)$ y $f^{-1}(x)$ en cada ítem del Ejercicio 7.

9. Encontrar las funciones inversas en cada una de las siguientes:

a) $x = y + b$
b) $x = by$
c) $x = cy + b$
d) $x = cy^n + b$
*e) $x = a^y$, en donde $0 < a$
*f) $x = \log_b y$, en donde $0 < b$.

10. Emplee la definición de $x^{1/n}$ que aparece en el Ejercicio 7 y defina $x^{m/n}$ para $x > 0$ y enteros cualesquiera m y n.

*El asterisco indica que el ejercicio incluye conceptos que no se han tratado en el presente texto, pero que debieran ser familiares a la mayoría de los lectores.

11. Una función $f(x)$ real uniforme es una *función creciente* de x en un intervalo $a < x < b$ si $f(x + h) - f(x) > 0$ para todo x y todo h tales que $a < x < x + h < b$. Demostrar que x^3 es una función creciente de x para $x > 0$.

12. Demostrar que x^n es una función creciente de x para $x > 0$ y cualquier entero positivo n. (*Indicación:* sea $x + h = y$; valerse del Ejercicio 7, Cap. I – 4).

13. Definir una función decreciente de x y demostrar que x^{-n} es una función decreciente de x para cualquier entero positivo n y $0 < x < 1$.

14. Demostrar que a^x es una función creciente de la variable positiva entera x cuando $a > 1$.

15. Repetir el Ejercicio 12, siendo n un entero cualquiera.

16. Demostrar que a^x es una función decreciente de la variable entera x para $0 < a < 1$.

17. Señalar, en el Ejercicio 7, las funciones que son funciones crecientes de la variable real y. Determínense los intervalos cuando sea necesario.

18. Señalar las funciones crecientes del Ejercicio 9.

III-11 L I M I T E S . Definiremos primero el límite de un conjunto ordenado de números reales

$$\{a_n\} = a_1, a_2, \ldots, a_n, \ldots$$

La notación $\{a_n\}$ indica que existe un número a_n correspondiente a cada entero positivo n, y que los números a_n (no necesariamente distintos) se consideran en el orden de sus subíndices. Por ejemplo, si $a_n = 1/n^2$, tenemos $a_1 = 1$, $a_2 = \frac{1}{4}$, $a_3 = \frac{1}{9}$, ... Tales conjuntos ordenados se llaman *sucesiones* de números. También estudiaremos sucesiones de funciones, tales como $\{x^n - 1\}$.

Las sucesiones:

$$1, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{1}{4}, \ldots, 1/n, \ldots,$$
$$-\tfrac{1}{2}, +\tfrac{1}{4}, -\tfrac{1}{8}, +\tfrac{1}{16}, \ldots, (-1)^n/2^n, \ldots,$$
$$.1, .01, .001, \ldots, 10^{-n}, \ldots$$

tienen, evidentemente, una propiedad común, porque para cada sucesión $\{a_n\}$ el término a_n puede elegirse arbitrariamente de modo de obtener un valor absoluto pequeño eligiendo valores de n suficientemente grandes. En otras palabras, $|a_n - 0|$ puede hacerse menor que cualquier número dado positivo ε, haciendo n tan grande como se quiera. Designaremos por N un valor particular de n tal que $|a_n - 0| < \varepsilon$ para todo $n \geqq N$. Puesto que $|a_n| > |a_{n+1}|$ en cada una de las sucesiones dadas, resulta evidente que $|a_n$

$- 0| < \varepsilon$ para $n = N$ implica que se satisface también la misma relación para cualquier $n \geq N$. En la terminología del análisis, se denota la dependencia de N respecto de ε escribiendo N_ε. Por ejemplo, si $\varepsilon = 1$ y $\{a_n\} = \{1/n\}$, entonces podemos elegir $N_1 = 2$. Si $\varepsilon = .01$ para la misma sucesión, elegimos $N_{.01} = 101$. La necesidad de esta dependencia de N respecto del ε dado resulta evidente porque para cualquier valor dado de N, se podría elegir un ε tal que el N dado no satisfaga las condiciones pedidas. En particular, si $\{a_n\} = \{1/n\}$ y $N = 1,\ 658,\ 972$ es dado, se necesita sólo hacer $\varepsilon = 10^{-7}$ para probar que ε debe darse primero y N_ε elegirse respecto del ε dado. Usando esta terminología, podemos describir la propiedad común de las sucesiones anteriores diciendo que dado cualquier número positivo ε, existe un entero N_ε tal que $|a_n - 0| < \varepsilon$ para todo $n \geq N_\varepsilon$. Se dice que las sucesiones que tienen esta propiedad se aproximan a cero como límite y de aquí que sean llamadas *sucesiones nulas*.

Si consideramos las sucesiones:

$$.9,\ .99,\ .999,\ \ldots,\ (10^n - 1)\ /10^n,\ \ldots,$$

$$\tfrac{2}{1},\ \tfrac{3}{2},\ \tfrac{4}{3},\ \ldots,\ (n+1)\ /n,\ \ldots,$$

encontraremos que en cada sucesión los términos a^n tienden a 1 a medida que n aumenta. Dado $\varepsilon = .1$, podemos hacer $N_\varepsilon = 2$ en la primera sucesión y $N_\epsilon = 11$ en la segunda sucesión para obtener $|a_n - 1| < \varepsilon = .1$ para todo $n \geq N_\varepsilon$. Asimismo, si $\varepsilon = .001$. podemos hacer $N_\varepsilon = 4$ en la primera sucesión y $N_\varepsilon = 1001$ en la segunda sucesión. En general, se dice que *una sucesión de números*

$$a_1,\ a_2,\ \ldots,\ a_n\ \ldots$$

tiende a un límite finito A, $\lim_{n\to\infty} a_n = A$, *si para todo número positivo* ε *existe un entero* N_ε *tal que para cualquier* $n \geq N_\varepsilon$ *se satisfaga la desigualdad* $|a_n - A| < \varepsilon$.

Pueden definirse muchas sucesiones tales como $\{n\}$ y $\{-n^2\}$ que tienden a límites infinitos (Ejercicio 8) (ver Bibliografía Nº 12, pág. 33). Muchas otras sucesiones, tales como $\{(-1)^n\}$ y $\{n(-1)^n\}$, oscilan y no tienden a ningún límite. No consideraremos tales su-

cesiones, dado que necesitaremos solamente *sucesiones convergentes*, es decir, sucesiones que tiendan a un límite finito. Un buen estudio general de sucesiones puede consultarse en (Bibliografía Nº 12, págs. 27-41).

Las manipulaciones de las desigualdades numéricas que se emplean en la determinación de N_ε para una sucesión dada, se basan sobre las definiciones del Cap. 1, Secciones 6, 9 y 12. En resumen dado $a < b$, resulta para cualquier número real c

$$a + c < b + c,$$

y, por lo tanto,

$$a - c < b - c.$$

También

$$ac < bc \text{ si } c \text{ es positivo,}$$
$$ac > bc \text{ si } c \text{ es negativo.}$$

La convergencia de una sucesión puede considerarse también con respecto de las sucesiones de Cauchy. Una sucesión de números reales $\{a_n\}$ se llama una *sucesión de Cauchy* si para cualquier número dado positivo ε existe un entero N_ε tal que $|a_n - a_{n-k}| < \varepsilon$ para $n \geqq N_\varepsilon$ y para todo entero positivo k. El criterio de convergencia de Cauchy (Ejercicio 4) establece, entonces que toda sucesión de Cauchy es una sucesión convergente y, a la inversa, que toda sucesión convergente es una sucesión de Cauchy. En consecuencia, puede probarse que una sucesión es convergente demostrando que es una sucesión de Cauchy.

Todas las sucesiones precedentes se obtuvieron expresando a_n como una función de la variable positiva entera n y considerando la sucesión de valores de a_n para $n = 1, 2, \ldots$. También podemos obtener sucesiones expresando el término general, por ejemplo, a_x, como una función de una variable real continua x y considerando la sucesión de valores de a_x que corresponden a cualquiera sucesión de números reales elegidos como valores de x. Por ejemplo, sea $a_x = x + 5$ y elijamos para x los valores $1, 1/\sqrt{2}, 1/\sqrt{3}, \ldots, 1/\sqrt{n}, \ldots$. Nos serviremos de este concepto en las dos secciones que siguen de este capítulo para definir una función continua y una variable continua.

EJERCICIOS

1. Demostrar que las sucesiones siguientes son sucesiones nulas:

$$1,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \frac{1}{5},\ \ldots,\ \frac{1}{n},\ \ldots,$$

$$\frac{1}{2},\ -\frac{1}{4},\ \frac{1}{8},\ -\frac{1}{16},\ \frac{1}{32},\ \ldots,\ \frac{(-1)^{n+1}}{2^n},\ \ldots,$$

$$.1,\ .01,\ .001,\ .0001,\ \ldots,\ \frac{1}{10^n},\ \ldots.$$

2. Escribir los primeros cinco términos y encontrar el límite de cada una de las siguientes sucesiones:

a) $\{n^{-2}\}$; b) $\{[5n + (-1)^{n+1}]\, n\}$; c) $\{(n^3 - 1)/n^4\}$.

3. Determinar N_ε para cada una de las sucesiones del Ejercicio 2: (a) si ε es un número positivo arbitrario; (b) si $\varepsilon = .01$.

4. Demostrar el *criterio de convergencia de Cauchy:* una sucesión de números reales $\{a_n\}$ tiende a un límite finito A si y sólo si para cualquier número positivo dado ε existe un entero N_ε tal que $|a_n - a_{n+k}| < \varepsilon$ para $n \geqq N_\varepsilon$ y para todo entero positivo k. (Ver Bibliografía Nº 21; págs. 35-36).

5. Si $\lim_{n\to\infty} a_n = A$ y $\lim_{n\to\infty} b_n = B$, en donde A y B son números reales, demostrar que:

(a) $\lim_{n\to\infty} (a_n + b_n) = A + B$,

(b) $\lim_{n\to\infty} (a_n - b_n) = A - B$,

(c) $\lim_{n\to\infty} a_n b_n = AB$, y

(d) para $B \neq 0$, $\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{A}{B}$.

6. Para postular la existencia de los números reales suele utilizarse la suposición de que toda sucesión convergente de números racionales tiene un límite. En el Ejercicio 5, se ha señalado que los límites de las sucesiones de números pueden sumarse, restarse, multiplicarse y dividirse lo mismo que los números. Probar que las relaciones de orden para los límites de las sucesiones son análogas, pero no exactamente las mismas que las relaciones de orden para los números, demostrando que

a) si $a_n \geqq 0$ $\lim_{n\to\infty} a_n = A$, entonces $A \geqq 0$.

b) si $a_n \geqq b_n$, $\lim_{n\to\infty} a_n = A$, $\lim_{n\to\infty} b_n = B$, entonces $A \geqq B$.

c) es posible que sea $a_n > b_n$, $\lim_{n\to\infty} a_n = A$, $\lim_{n\to\infty} b_n = B$, y $A = B$.

7. Por medio del Ejercicio 10, Cap. III — 10, y de la definición de un número real como el límite de una sucesión de números racionales, definir x^b para cualquier número real positivo b.

8. Podemos definir los símbolos $\lim_{n\to\infty} a_n = +\infty$, $\lim_{n\to\infty} -a_n = -\infty$ si para cualquier $\varepsilon > 0$ existe un entero N_ε tal que $a_n > 1/\varepsilon$ para $n \geqq N_\varepsilon$. Siendo así, se dice que la sucesión $\{a_n\}$ se ha hecho positivamente infinita si para cualquier entero positivo dado p se tiene $a_n > p$ para todos los valores suficientemente grandes de n. Demostrar que si el $\lim_{n\to\infty} a_n = +\infty$, $\lim_{n\to\infty} b_n = B$, en donde B, es finito y el $\lim_{n\to\infty} c_n = 0$, entonces.

a) $\lim_{n\to\infty} (a_n \pm b_n) = +\infty$.

b) $\lim_{n\to\infty} (b_n - a_n) = -\infty$.

c) $\lim_{n\to\infty} \frac{b_n}{a_n} = 0$.

d) $\lim_{n\to\infty} a_n b_n = +\infty$ si $0 < B$.

(e) $\lim_{n\to\infty} \frac{b_n}{c_n} = +\infty$ si $0 < B$.

9. Utilizar los resultados del Ejercicio 8 para justificar las siguientes convenciones, en donde B es finito:

a) $\infty \pm B = \infty$,

b) $B - \infty = -\infty$,

c) $B / \infty = 0$,

d) $\infty \cdot B = \infty$ si $0 < B$,

e) $B/0 = \infty$ si $0 < B$.

Nótese que también hay algunas operaciones indefinidas respecto de los símbolos ∞ y 0: $\infty - \infty$; ∞/∞; $0/0$; $\infty \cdot 0$; 0^0; ∞^0 1^∞.

10. Dada una sucesión infinita $\{a_n\}$ de números reales, en donde n es una variable entera positiva, la suma indicada $\sum_{n=1}^{\infty} a_n$ se llama *serie infinita* de números

reales. La serie *converge* hacia (tiene una suma) S si y sólo si la sucesión de sumas parciales s_n en donde $s_n = a_1 + a_2 + \cdots + a_n$, tiene un límite S y S es finito. Se dice que la serie es *divergente* en todos los otros casos, es decir, cuando (i) $\{s_n\}$ se hace positivamente infinita; (ii) $\{s_n\}$ se hace negativamente infinita; (iii) $\{s_n\}$ oscila y por lo tanto S no existe. Proponer ejemplos que ilustren cada uno de estos tres casos de series divergentes.

11. Demostrar que si $\sum_{n=1}^{\infty} a_n = S$, $\sum_{n=1}^{\infty} b_n = R$ y C, es cualquier número real, entonces

$$\text{(a)} \quad \sum_{n=k}^{\infty} a_n = S - a_1 - a_2 - \cdots - a_{k-1},$$

$$\text{(b)} \quad C + \sum_{n=1}^{\infty} a_n = C + S,$$

$$\text{(c)} \quad \sum_{n=1}^{\infty} Ca_n = CS,$$

$$\text{(d)} \quad \lim_{n \to \infty} a_n = 0,$$

$$\text{(e)} \quad \sum_{n=1}^{\infty} (a_n + b_n) = S + R.$$

12. Exponer en palabras cada uno de los item del Ejercicio 11 e indicar su significado.

III - 12 CONTINUIDAD. Frecuentemente hemos oído decir que una curva continua es aquella que puede trazarse sin levantar el lápiz. Tales curvas son efectivamente continuas y esta definición es fácil de imaginar. Sin embargo, tal defi-

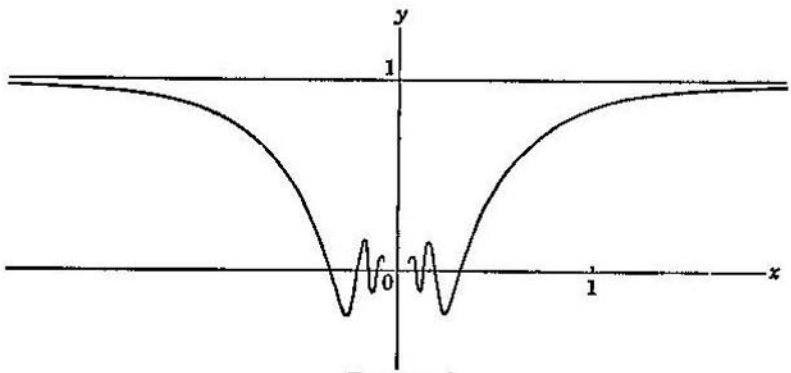


FIG. III—1

nición no es exacta, dado que existen curvas, tales como $y = x \operatorname{sen}(1/x)$ en las cercanías del origen, que oscilan tan rápidamente que no pueden trazarse con un lápiz (Fig. III-1), y sin embargo, algunas de estas curvas son también continuas. Una curva continua es el gráfico de una función continua y, a la inversa, el gráfico de una función continua es una curva continua. Nos serviremos de este hecho para definir la continuidad con respecto a los límites de las curvas y de las funciones.

Consideremos la función $y = f(x)$ cuyo gráfico aparece en la Fig. III-2. Esta función está determinada por

$$\begin{aligned} y &= 2 \text{ para } x < -1, \\ &= -x \text{ para } -1 \leqq x \leqq 0, \\ &= 1/x \text{ para } 0 < x. \end{aligned}$$

De este modo podemos asociar exactamente un valor de y con cada valor real de x para todos los números reales x. Siendo así (Cap. III-10), tenemos una función uniforme $y = f(x)$ de una variable real continua x.

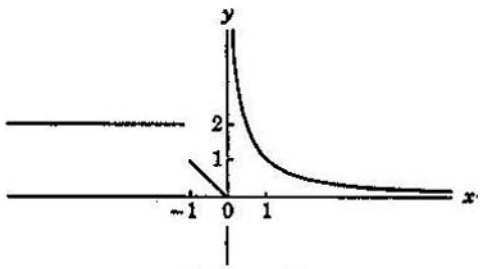


FIG. III—2

Del gráfico se desprende que la función es continua para los x positivos, pero no para todos los x. Examinemos ahora la curva más detalladamente y tratemos de encontrar un fundamento para describir una curva como continua.

Toda interrupción en la curva debe producirse en algún punto tal como $x = -1$ y $x = 0$ de la Fig. III-2. Por eso nos referiremos principalmente a la continuidad en un punto. Si una curva es continua en todos los puntos de un intervalo (Cap. III-10), se define como continua en ese intervalo. La curva en referencia parece ser y es continua en cada uno de los tres segmentos $x < -1$; $-1 < x < 0$; $0 < x$. Los puntos en los cuales la curva salta o se interrumpe se llaman puntos de *discontinuidad*. Estos puntos pueden definirse exactamente por medio de límites de sucesiones (Cap. III-13).

Supongamos que $y = f(x)$ está definida igual como en la Fig.

III-2. Para cualquier sucesión de números positivos $\{a_n\}$ que tiene un límite 2, existe una sucesión correspondiente $\{1/a_n\}$ de valores de $y = f(x)$. Se dice que la función $f(x)$ es continua en $x = 2$, puesto que para *toda* sucesión de valores de x que tenga el límite 2, la sucesión correspondiente de valores de $f(x)$ tiene el límite $\frac{1}{2}$ y $f(2) = \frac{1}{2}$. La función $f(x)$ es discontinua en $x = 0$, puesto que existen sucesiones nulas de valores de x tales que las sucesiones correspondientes de valores de $f(x)$ no tienden al mismo límite. En particular, si la sucesión de valores de x es $\{-1/n\}$, entonces la sucesión de valores de $f(x)$ en la Fig. III-2 es $\{1/n\}$ tiene límite cero. Si la sucesión de valores de x es $\{1/n\}$, entonces la sucesión de valores de $f(x)$ es $\{n\}$, que crece indefinidamente. Es así como existen sucesiones nulas de valores de x tales que las sucesiones correspondientes de valores de $f(x)$ no tienen el mismo límite. La función y la curva de la Fig. III-2 se llaman, en este caso, discontinuas para $x = 0$. En la Fig. III-1 toda sucesión nula de valores de x corresponde a una sucesión de valores nula de $y = x\text{sen}\,(1/x)$ y, suponiendo que $y = 0$ cuando $x = 0$, se dice que la curva es *continua* para $x = 0$.

De la Fig. III-2 resulta evidente que si x tiende a cero por medio de cualquier sucesión de valores negativos, la sucesión correspondiente de valores de $y = f(x)$ tiende a cero. Este límite común de todas las sucesiones de $f(x)$ que corresponden a sucesiones de valores de x que tienden a cero por el lado negativo se indica por medio de la notación $\lim_{x \to 0^-} f(x) = 0$. Análogamente, respecto de la Fig. III-2, diremos que $\lim_{x \to 0^+} f(x)$ es infinito, que el $\lim_{x \to 2^-} f(x) = \frac{1}{2}$, que el $\lim_{x \to 2^+} f(x) = \frac{1}{2}$, que el $\lim_{x \to -1^-} f(x) = 2$, $\lim_{x \to -1^+} f(x) = 1$. En la sección siguiente usaremos los conceptos de límite por la izquierda y límite por la derecha para definir una función continua.

EJERCICIOS

1. Hacer el gráfico (no se exigen condiciones algebraicas) de una función $f(x)$ tal que:

a) $\lim_{x \to 0^-} f(x) = -1$ y $\lim_{x \to 0^+} f(x) = +1$;

b) $\lim_{x \to 2^-} f(x) = 0$ y $\lim_{x \to 2^+} f(x) = 5$.

2. Por definición, $\lim_{x \to a} f(x) = f(a)$ si y sólo si $\lim_{x \to a^-} f(x) = \lim_{x \to a^+} f(x) = f(a)$. Hacer el gráfico de una función tal que $\lim_{x \to a} f(x) = f(a)$ para todo valor real de a.

3. Hacer el gráfico de una función tal que $\lim_{x \to a} f(x) \neq f(a)$ para $a = -2, 0, 2$.

4. Hacer el gráfico de una función tal que $\lim_{x \to 0^-} f(x) = 0$; $f(0) = 1$; y $\lim_{x \to 0^+} f(x) = 2$.

5. Hacer el gráfico de una función tal que $\lim_{x \to 0^-} f(x) = 0$; $f(0) = 1$, y $\lim_{x \to 0^+} f(x) = 0$.

III-13 FUNCIONES CONTINUAS. Cuando x es una variable real continua, se dice que una función uniforme $y = f(x)$ determinada para $a < x < b$, es *continua* para x_0, en que $a < x_0 < b$, si y sólo si $\lim_{x \to x_0^-} f(x) = f(x_0) = \lim_{x \to x_0^+} f(x)$. Como se señaló anteriormente, $f(x)$ es *continua en un intervalo* si es continua en *todos* los puntos del intervalo. En consecuencia, la función $f(x)$ es continua en un intervalo si y sólo si el límite por la izquierda, el límite por la derecha y el valor de la función son iguales en todos los puntos de ese intervalo.

Si los dos límites $\lim_{x \to x_0^-} f(x)$ y $\lim_{x \to x_0^+} f(x)$ son finitos e iguales, entonces o bien su límite común es $f(x_0)$ y $f(x)$ es continuo en $x = x_0$ o su límite común no es $f(x_0)$ y $f(x)$ tiene una *discontinuidad evitable* en $x = x_0$. Por ejemplo, la función:

$$\begin{aligned} f(x) &= 1 \qquad \text{cuando } x < 3, \\ &= 2 \qquad \text{cuando } x = 3, \\ &= 4 - x \text{ cuando } x > 3, \end{aligned}$$

está representada en la Fig. III-3. Hay una discontinuidad evitable en $x = 3$ que puede eludirse definiendo nuevamente $f(x)$, como sigue:

$$f(x) = 1 \quad \text{cuando } x \leqq 3,$$
$$= 4 - x \quad \text{cuando } x > 3.$$

Si los dos límites son finitos, pero no iguales, $f(x)$ tiene una discontinuidad en $x = x_0$ que se llama *salto finito*. Por ejemplo, en la Fig. III-2, $f(x)$ tiene un salto finito en $x = -1$.

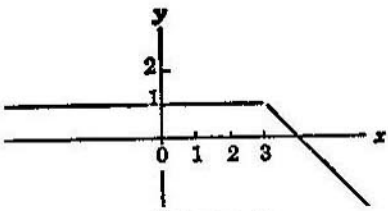


FIG. III—3

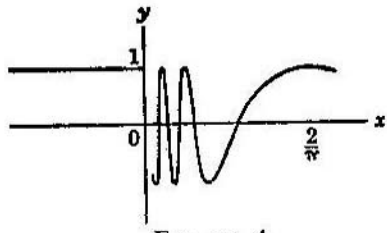


FIG. III—4

Si por lo menos uno de los límites no es finito, entonces o bien por lo menos un límite se hace infinito y $f(x)$ tiene una *discontinuidad infinita* o un límite oscila (no existe) y $f(x)$ es discontinua. Por ejemplo, en la Fig. III-2, $f(x)$ tiene una discontinuidad infinita en $x = 0$. Las funciones $y = 1/x$ y $1/x^2$ tienen también cada una discontinuidad infinita en $x = 0$. La función cuyo gráfico aparece en la Fig. III-4 está dada por:

$$f(x) = 1 \quad \text{cuando } x \leqq 0,$$
$$= \operatorname{sen}\ (1/x) \quad \text{cuando } x > 0.$$

Si $\{x\} = \{1/(n\pi)\}$, entonces $\{f(x)\} = \{0\}$ tiene límite 0; si $\{x\} = \{2/[(4n + 1)\pi]\}$ luego $\{f(x)\} = \{1\}$ tiene límite 1. En realidad, para cualquier b, $-1 \leqq b \leqq 1$, existe una sucesión nula de valores positivos de x tal que la sucesión correspondiente de valores de $f(x)$ tenga un límite b. En este caso, $\lim_{x \to 0^+} f(x)$ no existe y se dice que la curva y la función son discontinuas en $x = 0$.

Daremos ahora una segunda definición de una función continua, en la que se reemplaza el concepto de límite por algunos de los conceptos empleados en la definición de un límite. Aquí de nuevo un dibujo será una ayuda visual muy útil.

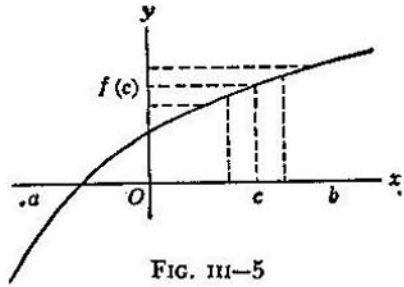


FIG. III–5

Una función uniforme $f(x)$ (Fig. III - 5) definida por $a \leqq x \leqq b$ es continua en $x = c$, en donde $a \leqq c \leqq b$ si y sólo si para cada $\varepsilon > 0$ existe un $\delta\ \varepsilon_c$ tal que $|f(x) - f(c)| < \varepsilon$ para todo x comprendido en $a \leqq x \leqq b$ que satisfaga $|x - c| < \delta\ \varepsilon_c$. La notación $\delta\ \varepsilon_c$ indica que δ depende del ε dado y del punto elegido $x = c$.

Si dos funciones $f(x)$ y $g(x)$ son continuas en $x = c$, entonces por definición, dado $\varepsilon > 0$, existe un valor positivo $\delta\ \varepsilon_c$ para $f(x)$ y otro para $g(x)$. El menor de estos dos números positivos satisfará las dos funciones $f(x)$ y $g(x)$ en $x = c$. Asimismo, si $f(x)$ y $g(x)$ son continuas, existe un $\delta\ \varepsilon_c$ tal que se verifica $|f(x) - f(c)| < \varepsilon$ y $|g(x) - g(c)| < \varepsilon$ para $|x - c| < \delta\ \varepsilon_c$. Aprovecharemos estas relaciones para demostrar que la suma $f(x) + g(x)$ de dos funciones continuas, es continua. Dado $\varepsilon > 0$, $\varepsilon/2$ será nuestro número positivo y elegiremos δ tal que para $|x - c| < \delta$, tengamos $|f(x) - f(c)| < \varepsilon/2$ y $|g(x) - g(c)| < \varepsilon/2$. Luego

$$[[f(x) + g(x)] - [f(c) + g(c)]| = |f(x) - f(c) + g(x) - g(c)| \leqq$$
$$|f(x) - f(c)| + |g(x) - g(c)| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Esto completa la demostración de que la suma de dos funciones continuas en un punto, es continua en ese punto. El conjunto siguiente de ejercicios requiere el método de demostración ya citado, y permite llegar a uno de los principales resultados de esta sección, es decir, al Ejercicio 4. La demostración de este ejercicio se desprende de los ejercicios precedentes, teniendo en cuenta que cada polinomio consta de una variable y de un conjunto de coeficientes combinados por medio de operaciones de anillo.

EJERCICIOS

1. Si $f(x)$ es continuo en $x = c$ y $g(x)$ es continuo en $x = c$, demostrar que $f(x) - g(x)$ es también continuo en $x = c$.

2. Si $f(x)$ y $g(x)$ son continuos en $x = c$, demostrar que $f(x) \cdot g(x)$ es también continuo en $x = c$.

3. Si $f(x)$ y $g(x)$ son continuos en un segmento $a < x < b$, demostrar que $f(x) + g(x)$, $f(x) - g(x)$, y $f(x) \cdot g(x)$ son continuos en ese mismo segmento.

4. Demostrar que cualquier polinomio en una variable real continua x con coeficientes reales es continuo para todos los valores reales de x.

5. Si existen números reales a y b, $a < b$, tales que $p(a) \cdot p(b) < 0$, en donde $p(x)$ es un polinomio real, demostrar que hay un número real c, $a < c < b$, tal que $p(c) = 0$. (Ver Bibliografía Nº 12; págs. 66-67).

6. Hacer el gráfico y discutir la continuidad de cada una de las siguientes funciones:

a) $y^2 = x^2 - 9$

b) $y = \sqrt{x^2 - 9}$

c) $y^2 = x^2$

d) $x^2y = 1$

e) $y = \dfrac{x^2 + 1}{x^2 - 1}$

f) $y = 2^x$

g) $y = 1$ para $x \leqq 0$
$\quad = x$ para $x > 0$

h) $y = |x|$ para $x \neq 0$
$\quad = 1$ para $x = 0$

7. Dibujar gráficos de funciones uniformes que ilustren cada uno de los casos siguientes:

a) discontinuidades evitables en $x = 0$ y $x = 1$;

b) discontinuidades finitas en $x = n$ para todos los enteros positivos n;

c) discontinuidades infinitas para $x = +1$ y $x = -1$.

8. Proponer expresiones algebraicas para funciones uniformes que cumplan con las condiciones pedidas en el Ejercicio 7.

9. Una función uniforme $f(x)$ definida en el intervalo $a \leqq x \leqq b$ es *uniformemente continua* en ese intervalo si y sólo si para todo $\varepsilon > 0$ existe un δ_ε tal que $|f(x) - f(x_0)| < \varepsilon$ para todo x y x_0 (cualquier valor determinado de x) en el intervalo dado que satisfaga $|x - x_0| < \delta_\varepsilon$. Hacer el gráfico de una función que sea continua en $0 < x < 1$ pero no uniformemente continua en $0 \leqq x \leqq 1$.

10. Demostrar (ver Bibliografía Nº 12; págs. 65-66) que si una función es continua en un intervalo cerrado, es uniformemente continua en ese intervalo.

11. Demostrar que si una función es continua en un intervalo cerrado: (a) está acotada en ese intervalo; (b) tiene un máximo M y un mínimo m en ese intervalo, y (c) adquiere cualquier valor b, por lo menos una vez en ese intervalo, siendo $m \leqq b \leqq M$.

12. Hacer el gráfico de una función $y = f(x)$ que sea uniforme, continua y creciente para $a \leqq x \leqq b$. Puede demostrarse que existe una función inversa correspondiente $x = f^{-1}(y)$ que es también uniforme, continua y creciente (ver Bibliografía Nº 12; págs. 67-68). Compruébense estas propiedades para la función representada en el gráfico.

13. Valiéndose del resultado expuesto en el Ejercicio 12, demostrar que $y^{1/n}$

puede definirse como una función creciente de y, uniforme y continua, en donde $y > 0$ y n es cualquier entero positivo (ver Ejercicio 12, Cap. III-10).

14. Para $a > 1$ demostrar que a^x es una función creciente de la variable positiva real x (ver Ejercicio 7, Cap. III-11).

15. Demostrar que $\log_a y$ puede determinarse como una función creciente, uniforme y continua de y, en que $y > 0$ y $a > 1$.

III - 14 DERIVADAS. Las derivadas de un polinomio $p(x)$ pueden definirse mediante límites o simplemente por medio de los coeficientes del polinomio $p(x + h)$. Si $p(x) = x^2$, entonces $p(x + h) = x^2 + 2xh + h^2$. El coeficiente de h en $p(x + h)$ puede considerarse como la primera derivada de $p(x) = x^2$. Se escribe $(d/dx)\, p(x) = p'(x) = (x^2)' = 2x$. En general, la derivada de cualquier polinomio $p(x)$ puede considerarse como el coeficiente de h en el desarrollo de $p(x + h)$.

La *derivada* con respecto a x de cualquier polinomio $p(x)$ se define comúnmente como

$$p'(x) = \lim_{h \to 0} \frac{p(x + h) - p(x)}{h},$$

puesto que este límite existe en los polinomios para todos los valores reales de x y esta definición puede hacerse extensiva fácilmente a funciones más generales. La derivada en $x = x_0$ (un valor determinado de x) de una función $f(x)$ uniforme arbitraria se define por

$$f'(x_0) = \lim_{h \to 0} \frac{f(x_0 + h) - f(x_0)}{h}$$

siempre que el límite exista. Cuando el límite no existe, la derivada es indefinida.

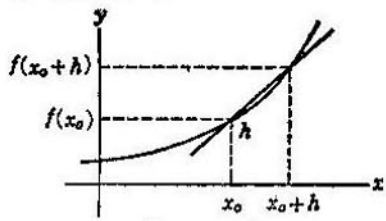


FIG. III—6

Geométricamente, la definición precedente de la derivada de $f(x)$ puede representarse por medio de la tangente y la secante en el gráfico de $f(x)$. Cualquiera recta que corte el gráfico de $f(x)$ en dos puntos puede llamarse recta secante o *secante*. En particular, consideraremos una secante (Fig. III-6) que corte el gráfico de $f(x)$ en $[x_0, f(x_0)]$ y $[x_0 + h, f(x_0 + h)]$. La pendiente de esta recta puede considerarse como

$$\frac{f(x_0 + h) - f(x_0)}{h}.$$

La recta tangente o *tangente* al gráfico de $f(x)$ en $[x_0, f(x_0)]$ puede definirse como la posición límite de la secante señalada a medida que h tiende a cero. De aquí que la pendiente de la tangente en $x = x_0$, sea el límite de la pendiente de la secante, a medida que h tiende a cero y es precisamente la derivada de $f(x)$ en $x = x_0$.

La derivada está indefinida en todos los puntos de discontinuidad y en los puntos de una curva en la cual la pendiente de la tangente sea una función discontinua de la variable independiente. Por ejemplo, si

$$\begin{aligned} f(x) &= x \qquad \text{cuando } x \leqq 1, \\ &= 2 - x \text{ cuando } x > 1, \end{aligned}$$

tenemos el gráfico de la Fig. III - 7. En $x = 1$ la pendiente de la tangente cambia abruptamente de 1 a -1 y la derivada en $x = 1$ es indefinida.

Dado cualquier monomio bx^n, se puede obtener

$$b(x + h)^n = b[x^n + nhx^{n-1} + \frac{n(n-1)}{1 \cdot 2} h^2 x^{n-2} + \cdots + h^n].$$

De este modo nbx^{n-1} es la derivada de bx^n sea que la derivada se considere como un límite o como el coeficiente de h. En seguida observaremos que $[f(x) + g(x)]'$ puede considerarse como el coeficiente de h en $[f(x + h) + g(x + h)]$, es decir, $[f(x) + g(x)]' = f'(x) + g'(x)$. En otras palabras, la derivada de la suma de dos funciones es igual a la suma de las derivadas de las funciones. En particular, considerando un polinomio como una suma de monomios, la derivada de un polinomio es igual a la suma de las derivadas de sus términos (monomios). Dado que cualquier monomio bx^n tiene una derivada nbx^{n-1}, la derivada de cualquier polinomio

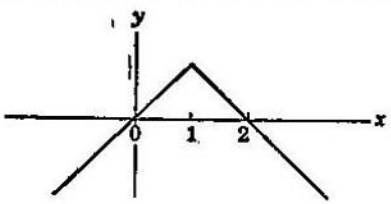


FIG. III—7

$$p(x) = a_n + a_{n-1}x + a_{n-2}x^2 + a_{n-3}x^3 + \cdots + a_0x^n$$

resulta

$$p'(x) = a_{n-1} + 2a_{n-2}x + 3a_{n-3}x^2 + \ldots na_0x^{n-1}.$$

De este modo encontraremos la primera derivada $p'(x)$ con respecto a x de cualquier polinomio $p(x)$. Dado que $p'(x)$ es también un polinomio, puede repetirse el procedimiento para obtener $p''(x)$, la derivada de $p'(x)$ con respecto a x,

$$p''(x) = 2a_{n-2} + 3 \cdot 2a_{n-3}x + \ldots + n(n-1)a_0x^{n-2}.$$

Análogamente, se puede obtener $p'''(x)$, $p^{(4)}(x)$, $\ldots$, $p^{(n)}(x)$. Y por último, $p^{(n+k)}(x) = 0$ para cualquier entero positivo k, ya que la derivada de una constante es igual a cero. Hablaremos de $p^{(r)}(x)$, en donde r es cualquier entero positivo, al referirnos a la r-ésima derivada de $p(x)$.

Los valores de $p(x)$ y sus primeras n derivadas cuando $x = 0$ están estrechamente relacionadas con los coeficientes de $p(x)$. Por ejemplo, en $x = 0$, tenemos $p(0) = a_n$, $p'(0) = a_{n-1}$, $p''(0) = 2a_{n-2}$, $p'''(0) = 3(2a_{n-3})$, $\ldots$, $p^{(n)}(0) = n!(a_0)$. Si estas ecuaciones se resuelven respectivamente para a_n, a_{n-1}, a_{n-2}, $\ldots$, a_0, y se sustituyen las expresiones correspondientes por los coeficientes del polinomio $p(x)$, tenemos

$$p(x) = p(0) + p'(0)x + \frac{p''(0)}{2!}x^2 + \frac{p'''(0)}{3!}x^3 + \cdots + \frac{p^{(n)}(0)}{n!}x^n.$$

Este método de expresar un polinomio $p(x)$ por medio de sus derivadas en un punto (en el caso anterior en $x = 0$) es un caso especial de la *fórmula de Taylor* para los polinomios:

$$p(x) = p(a) + p'(a)(x-a) + \frac{p''(a)}{2!}(x-a)^2 + \cdots + \frac{p^{(n)}(a)}{n!}(x-a)^n.$$

Esta fórmula puede aplicarse para expresar cualquier polinomio $p(x)$ por medio de los valores del polinomio y de sus derivadas en $x = a$, para cualquier número real a. También proporciona un método efectivo de expresar $p(x)$ en la forma $q(x + h)$, en donde $a = -h$, es decir, reemplazando la variable x por la nueva variable $x + h$ (Cap. III - 8).

Hemos visto que dado cualquier polinomio $p(x)$ de grado n, podemos obtener su k-ésima derivada para cualquier entero positivo k. También para un polinomio $p(x)$ de grado n, hay máximo $n + 1$ términos en su fórmula de Taylor, dado que $p^{(n+k)}(x) = 0$ para todo entero positivo k. Sin embargo, existen funciones tales como $f(x) = e^x$ para las cuales no se anula ninguna derivada en $x = a$. En estos casos la fórmula de Taylor se amplía en la serie de Taylor (Cap. III - 15).

Ya hemos examinado todas las propiedades de los polinomios que necesitaremos en el Capítulo IV. Las propiedades del anillo de polinomios que corresponden a las propiedades del anillo de los enteros, el hecho de que todo polinomio en una variable real continua sea continuo y la expresión de cualquier polinomio por medio de sus derivadas empleando la fórmula de Taylor, nos servirán en nuestros estudios futuros.

Pondremos fin al presente capítulo con un breve examen de la serie de Taylor y de las funciones analíticas. Estos dos conceptos son muy importantes en matemáticas superiores, pero no son necesarios para nuestros estudios ulteriores. El papel fundamental de las funciones analíticas se evidencia en las correspondencias entre los números y las funciones que se tratan al final del Capítulo III - 10.

EJERCICIOS

1. Derivar la fórmula de Taylor cuando $a \neq 0$.
2. Escribir $p(x) = x^3 - 5x^2 + 3x - 2$ en la forma de $q(x - 1)$.
3. Escribir $p(x) = x^6 + 8x^7 - 6x^6 + 5x^3 + 3$ en la forma de $q(x + 1)$.
4. Repetir los Ejercicios 1, 2 y 3 del Cap. III-8, aplicando la fórmula de Taylor.
5. Proponer una función uniforme de x que sea continua para todos los valores de x pero que no tenga derivada en $x = 0$.
6. Demostrar que si $f(x)$ es una función creciente y $f'(x)$ existe en el intervalo $a < x < b$, entonces $f'(x) \geqq 0$ en $a < x < b$.
7. Hacer el gráfico de una función creciente $f(x)$ en el intervalo $a < x < b$, en donde $f'(d) = 0$ para algún $x = d$, en que $a < d < b$.

III - 15* SERIE DE TAYLOR. Dado un polinomio $p(x)$ de grado m, podemos suponer (Cap. III - 8) que $p(x)$ puede expresarse en la forma

$$p(x) = b_0 + b_1(x - a) + \ldots + b_m(x - a)^m.$$

Podemos en seguida determinar los b por medio del valor de $p(x)$ y sus derivadas en $x = a$ como en la fórmula de Taylor (Cap. III - 14). Se necesitan sólo $(m + 1)$ términos, ya que $p(x)$ tiene a lo más m derivadas diferentes de cero.

Dada cualquier función uniforme $f(x)$, podemos intentar expresarla en la forma

$$f(x) = b_0 + b_1(x - a) + b_2(x - a)^2 + \ldots, \qquad \text{(III - 4)}$$

en donde existe un término asociado con todas las potencias enteras, no negativas de $(x - a)$. Tal expresión se llama *serie infinita* y corresponde en cierto modo a un decimal infinito de nuestro sistema de números. Si $f(x)$ puede expresarse de la manera anterior, los b pueden expresarse nuevamente por medio de los valores de $f(x)$ y sus derivadas en $x = a$. Por ejemplo, $b_0 = f(a)$, $b_1 = f'(a)$, $b_2 = f''(a)/2$. Por eso una función debe tener derivadas de todos los órdenes si se desarrolla como en (III - 4). Cuando los b de (III - 4) se reemplazan por las expresiones correspondientes de $f(x)$ y sus derivadas en $x = a$, obtenemos la *serie de Taylor*:

$$f(x) = f(a) + f'(a)(x - a) + \cdots + \frac{f^{(n)}(a)(x - a)^n}{n!} + \cdots.$$

En general, dada cualquiera función uniforme $f(x)$ definida en un intervalo $c < x < d$, en donde $c < a < d$, podemos considerar, respectivamente $f(a)$, $f'(a)$, $f''(a)$, $\ldots$, $f^{(n)}(a)$, $\ldots$ Si $f^{(n)}(a)$ existe para todos los valores enteros positivos de n, entonces $f(x)$ tiene un desarrollo en serie de Taylor en $x = a$, como se señaló anteriormente.

Ahora podemos obtener la serie infinita que usamos en el Cap. I - 16. En todos los textos de cálculo se demuestra que la derivada de e^x es e^x, que la derivada de sen x es cos x y que la derivada de cos x es —sen x. Utilizando $f(x) = e^x$, $f'(x) = e^x$, y la serie de Taylor en $x = 0$, tenemos $f^{(n)}(0) = 1$ para todo entero positivo n y

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots.$$

Cuando $f(x) = \text{sen } x$, se tiene $f'(x) = \cos x$, $f''(x) = -\text{sen } x$, $f'''(x) = -\cos x$, $f^{(4)}(x) = \text{sen } x$, $\ldots$ En $x = 0$, $f(x) = f''(x) = f^{(iv)}(x) =$

0 y $f'(x) = 1$, $f'''(x) = -1$, $f^{(2k+1)}(x) = (-1)^k$ para cualquier entero positivo k. En seguida, obtenemos el desarrollo de la serie de Taylor:

$$\text{sen } x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots$$

El desarrollo de la serie de Taylor para cos x puede obtenerse de manera análoga. (Ejercicio 1).

Hemos indicado sistemáticamente cómo obtener un desarrollo de la serie de Taylor en $x = a$ para cualquier función que tenga derivadas de todos los órdenes en $x = a$. Dejaremos a los textos de análisis el asunto de la convergencia de las series infinitas, es decir, para qué valores de x la serie es significativa (ver Bibliografía Nº 12; págs. 320-329, 365-424). Las series para e^x y sen x convergen para todos los valores reales de x. Nuestro interés en el desarrollo sistemático se evidenciará cuando definamos una función analítica.

EJERCICIOS

1. Desarrollar una serie de Taylor para cos x con respecto a potencias de x.
2. Por medio de los desarrollos de cos x y sen x en serie de Taylor, encontrar un desarrollo en serie de Taylor cos $x + i$ sen x.
3. Desarrollar en serie de Taylor e^{ix} y compararla con la encontrada en el Ejercicio 2.

III - 16* FUNCIONES ANALITICAS. Completaremos ahora nuestro estudio de las correspondencias entre los números y las funciones que mencionamos en el Cap. III - 10. En el Cap. III - 1 definimos un polinomio y en las secciones 1 a 9 del Cap. III hemos hecho notar las correspondencias entre polinomios y enteros. En el Cap. III - 3 establecimos la correspondencia entre números racionales y funciones racionales. Ahora examinaremos brevemente las correspondencias mencionadas en el Cap. III que aún no se han considerado.

Se dice que un número es algebraico si satisface una ecuación polinomia con coeficientes enteros que no es idéntica a cero (Cap. I - 10). Se dice que todos los demás números son trascendentes. Análogamente, se dice que una función $y = f(x)$ es una *función algebraica* de x si satisface una ecuación polinomia con polinomios

en x como coeficientes y que no sea idéntica a cero en y. Por ejemplo, $y = \sqrt[3]{x}$ satisface $y^3 - x = 0$, y por lo tanto es una función algebraica. Todas las funciones que no son algebraicas se llaman *funciones trascendentales*. Por ejemplo, sen x, log x, y e^x son funciones trascendentes.

En el Cap. I - 10 obtuvimos los números reales suponiendo que todos los decimales son números. El conjunto de números reales también pudo haberse obtenido suponiendo que toda sucesión de Cauchy de números racionales representa un número real. Ahora obtendremos funciones analíticas de una variable x suponiendo que toda serie de Taylor en x representa una función. Muchos textos definen una *función analítica* de una variable x como una función que tiene un desarrollo en serie de Taylor. Aquí, como en la sección 15 de este Cap. III, se presenta el problema de la convergencia de la serie. En los enunciados anteriores se supone que un desarrollo de la serie de Taylor existe si y sólo si tiene un significado en algún segmento $a < x < b$.

Ya hemos visto que los polinomios forman no sólo un anillo con propiedades muy análogas a aquellas del anillo de los enteros, sino también que el conjunto de polinomios puede ampliarse en el conjunto de funciones analíticas de una manera muy análoga a aquella usada cuando se ampliaron los enteros hacia el conjunto de los números reales. Consideraremos más propiedades de los polinomios en nuestro estudio de la teoría de las ecuaciones polinomias en el Capítulo IV.

EJERCICIOS

1. Hacer una lista de diez funciones racionales de x y determinar los valores de x para los cuales cada función está definida (Cap. III-3).

2. Hacer una lista de diez funciones algebraicas y proponer ecuaciones polinomias que satisfagan a cada una de ellas.

3. Hacer una lista de diez funciones trascendentes.

CAPITULO IV

Teoría de las ecuaciones

Hemos estudiado previamente las operaciones, los monomios y las relaciones que se usan en la formación de polinomios. En este capítulo consideraremos ecuaciones $p(x) = 0$ que se obtienen al igualar a cero un polinomio en una variable. Por ejemplo, la ecuación polinomia $x^2 - x - 6 = 0$ se satisface cuando $x = 3$, ó $x = -2$. Esta ecuación establece una condición para la variable y se llama *ecuación condicional*. La ecuación $(x - 1)^2 = x^2 - 2x + 1$ es una identidad (Cap. III-4) y se satisface para todos los valores numéricos de la variable x. Nos preocuparemos principalmente de los métodos para determinar aquellos números que, al sustituir a x en la ecuación $p(x) = 0$, satisfacen la igualdad. Tales números se llaman *ceros* del polinomio o *raíces* de la ecuación. También suelen llamarse *soluciones* de la ecuación. Los temas que se tratan en este capítulo se han seleccionado con el objeto de preparar al lector para:

(i) encontrar todas las soluciones enteras y racionales de cualquiera ecuación polinomia dada, en una variable, con coeficientes racionales;

(ii) encontrar todas las soluciones de cualquiera ecuación polinomia dada con coeficientes complejos, siempre que sea posible, empleando radicales y las cuatro operaciones racionales.

(iii) determinar en cualquier intervalo dado el número exacto de soluciones reales de cualquiera ecuación polinomia dada con coeficientes reales, y

(iv) aproximar tanto como se desee cualquiera solución real de una ecuación polinomia dada con coeficientes reales.

IV-1 CEROS DE UN POLINOMIO. Hemos definido un número b como un cero del polinomio $p(x)$ si y sólo si $p(b) = 0$. Dado cualquier polinomio $p(x)$ y un número b, buscaremos las condiciones necesarias y suficientes para que $p(b) = 0$. Por supuesto que una de estas condiciones se obtendría por sustitución inmediata de b por x en el polinomio para obtener el número $p(b)$ y observar si este número es o no cero. Sin embargo, existe otra condición necesaria y suficiente (Teorema IV-1) que suele ser mucho más fácil de aplicar (Cap. IV-2) que la sustitución directa.

Dado un polinomio $p(x)$ y un número b, podemos encontrar por división un polinomio $q(x)$ y una constante R tal que

$$p(x) = (x - b) \cdot q(x) + R, \tag{IV-1}$$

como lo determina el Algoritmo de la División (Cap. III-5) para polinomios en una variable. La identidad (IV-1) da $p(b) = R$ para $x = b$. A veces, se alude a esta relación con el nombre de

TEOREMA DEL RESIDUO. *Si se divide $p(x)$ por $x - b$, el residuo es $p(b)$.*

De la identidad (IV-1) podemos obtener también el teorema siguiente:

TEOREMA IV-1. TEOREMA DEL FACTOR: *un polinomio $p(x)$ se hace 0 para $x = b$ si y sólo si es divisible por $x - b$.*

En otras palabras, la ecuación polinomia $p(x) = 0$ tiene una raíz $x = b$ si y sólo si el polinomio $p(x)$ tiene un divisor o factor $x - b$, es decir, si y sólo si $R = 0$ en la identidad (IV-1). La tarea de encontrar R y $q(x)$ en (IV-1) suele efectuarse más rápida y fácilmente por medio de una división sintética.

EJERCICIOS

1. Proponer tres ejemplos del Teorema del Residuo en que $p(x)$ tenga por lo menos grado tres.

2. Repetir el Ejercicio 1 para el Teorema del Factor.
3. Proponer cuatro ecuaciones condicionales.
4. Proponer tres ecuaciones que sean identidades.

IV-2 DIVISION SINTETICA. La división sintética, así como el esquema usado para encontrar el máximo común divisor de dos enteros (Cap. II - 5), proporciona un método elemental y conciso para dar a conocer los resultados de los cálculos algebraicos.

Supongamos que se nos da un número b y un polinomio de grado $n > 0$, por ejemplo,

$$p(x) = b_0x^n + b_1x^{n-1} + \ldots + b_n. \tag{IV - 2}$$

Entonces el polinomio $q(x)$ de (IV - 1) debe tener grado $n - 1$ y por eso debe ser de la forma

$$q(x) = c_0x^{n-1} + c_1x^{n-2} + \ldots + c_{n-1},$$

en donde hay que determinar los coeficientes c. La identidad (IV - 1) entonces toma la forma

$$b_0x^n + b_1x^{n-1} + \ldots + b_n \equiv c_0x^n + (c_1 - c_0b)x^{n-1} + \ldots + (c_{n-1} - c_{n-2}b)x + R - c_{n-1}b. \tag{IV - 3}$$

Si $x = 0$, (IV - 3) toma la forma $b_n = R - c_{n-1}b$. Si estos términos constantes iguales se restan de ambos miembros de (IV - 3) y si se divide por x ambos miembros de la ecuación que resulta, al hacer nuevamente $x = 0$, encontramos que $b_{n-1} = c_{n-1} - c_{n-2}b$. En general, los coeficientes de potencias iguales de x deben ser iguales, y entonces, se tiene

$$\begin{aligned} b_0 &= c_0, \\ b_1 &= c_1 - c_0b, \\ b_2 &= c_2 - c_1b, \\ &\cdot \\ &\cdot \\ &\cdot \\ b_{n-1} &= c_{n-1} - c_{n-2}b \\ b_n &= R - c_{n-1}b. \end{aligned}$$

Estas ecuaciones pueden resolverse con respecto a los c de modo que resulte

$$\begin{aligned} c_0 &= b_0, \\ c_1 &= b_1 + c_0 b, \\ c_2 &= b_2 + c_1 b, \\ &\cdot \\ &\cdot \\ &\cdot \\ c_{n-1} &= b_{n-1} + c_{n-2} b, \\ R &= b_n + c_{n-1} b, \end{aligned}$$

Y así sucesivamente determinar los coeficientes de $q(x)$ y R.

Las relaciones anteriores pueden expresarse muy concisamente por medio del siguiente esquema, es decir, por *división sintética*.

$$\begin{array}{llllll|l} b_0 & b_1 & b_2 & \dots & b_{n-1} & b_n & b \\ 0 & c_0 b & c_1 b & \dots & c_{n-2} b & c_{n-1} b & \\ \hline c_0 & c_1 & c_2 & \dots & & & \end{array}$$

En este esquema la primera fila contiene los coeficientes de $p(x)$ (incluso todos los coeficientes cero); el primer elemento de la segunda fila es cero y cada elemento siguiente es el producto del número b por el elemento de la tercera fila en la columna inmediatamente precedente; cada elemento de la tercera fila es la suma de los elementos de la misma columna que están encima de él. Por ejemplo, si $p(x) = x^3 - 3x^2 + 7x - 10$ y $b = 4$, el esquema anterior sería

$$\begin{array}{cccc|c} 1 & -3 & 7 & -10 & 4 \\ 0 & 4 & 4 & 44 & \\ \hline 1 & 1 & 11 & 34 & \end{array}$$

por lo tanto, $q(x) = x^2 + x + 11$ y $R = 34$, es decir, $x^3 - 3x^2 + 7x - 10 = (x - 4)(x^2 + x + 11) + 34$. Dado que el primer elemento, cero, de la segunda fila es siempre el mismo, frecuentemente no se escribe.

El esquema anterior para la división de un polinomio $p(x)$ por un polinomio primitivo lineal $x - b$ puede modificarse para

el caso de la división de $p(x)$ por un polinomio de segundo grado o de mayor grado en x. (Ver Bibliografía Nº 47; págs. 56-58). En general, la división sintética es muy útil para comprobar que $p(b) = 0$ en la forma señalada anteriormente; para expresar $p(x)$ en la forma $q(x - b)$, es decir, disminuyendo en b, los valores de los ceros (Cap. III - 8 y Cap. IV - 3); para resolver ecuaciones cúbicas y cuárticas (Cap. IV, Secciones 9 y 10); para calcular una tabla de valores con el objeto de hacer el gráfico de $y = p(x)$; para determinar una cota superior para los ceros de $p(x)$ (Cap. IV-11); y para resolver ecuaciones numéricas (Cap. IV - 13).

EJERCICIOS

1. Sin efectuar la división, encontrar el resto si
a) se divide $x^2 - 5x + 6$ por $x - 4$,
b) se divide $x^3 - 3x^2 + 6x - 5$ por $x - 3$,
c) se divide $x^4 - 3x^3 - 2x - 4$ por $x + 3$.

2. Sin efectuar la división, demostrar que
a) $13x^{19} + 14x^5 + 1$ es divisible por $x + 1$;
b) $2x^4 - x^3 - 6x^2 + 4x - 8$ es divisible por $x - 2$ y por $x + 2$;
c) $v^4 - 3v^3 + 3v^2 - 3v + 2$ es divisible por $v - 1$ y por $v - 2$;
d) $x^n - 1$ es divisible por $x - 1$.

3. Por medio de la división sintética, encontrar el cuociente y el resto:
a) dividiendo $2x^4 + 4x^3 - x^2 - 16x - 12$ por $x + 4$;
b) dividiendo $3x^4 - 27x^3 + 14x + 120$ por $x - 6$;
c) dividiendo $x^4 - 4x^3 - 8x + 32$ por $x - 4$.

4. Dado el polinomio $p(x) = x^3 - x^2 - 4x - 6$ que tiene un cero para $x = 3$, encontrar un polinomio cuadrático que tenga como ceros los otros dos ceros de $p(x)$.

5. Por medio de la división sintética escribir cada uno de los siguientes polinomio en la forma (IV-1):

a) $p(x) = x^6 - 3x^5 + 2x + 1$, $b = 1$;
b) $p(x) = x^6 - x^5 + 2x^3 - 77$, $b = -1$;
c) $p(x) = x^7 - 7x^4 + 3x^2 - 5x^2 + 6$, $b = 5$;
d) $p(y) = y^6 + 4y^3 + 2$, $b = -3$;
e) $p(y) = y^6 + 1$. $b = -2$.

IV - 3 CAMBIO DE VARIABLE. En el Cap. III-8 demostramos que cualquier polinomio $p(x)$ puede expresarse en la forma $q(x - b)$. En esta sección veremos cómo se puede utilizar la división sintética para encontrar el polinomio $q(x - b)$

cuando se han dado el polinomio $p(x)$ y un número b. En el Cap. III-14, ya se ha tratado un método, mediante la fórmula de Taylor.

Dado un polinomio $p(x)$ de grado m y un número b, podemos expresar $p(x)$ en la forma (Teorema III - 4):

$$(\text{IV} - 4)\quad p(x) = a_0 + a_1(x - b) + a_2(x - b)^2 + \ldots + a_m(x - b)^m,$$

en donde hay que determinar los a. Entonces

$$p(x) = (x - b)[a_1 + a_2(x - b) + \ldots + a_m(x - b)^{m-1}] + a_0$$
$$= (x - b) \cdot q_1(x) + a_0,$$

como en (IV-1). De este modo $a_0 = p(b)$ puede calcularse por división sintética como en el Cap. IV - 2. En seguida escribimos

$$q_1(x) = (x - b)[a_2 + a_3(x - b) + \ldots + a_m(x - b)^{m-2}] + a_1$$
$$= (x - b) \cdot q_2(x) + a_1,$$

de donde $a_1 = q_1(b)$. Este procedimiento puede continuarse hasta que resulte $a_2 = q_2(b)$, ..., $a_m = q_m(b)$ y de esta manera determinar completamente los coeficientes a en (IV - 4), es decir, determinar completamente $q(x - b) = p(x)$.

Supongamos que $p(x) = x^4 - x^3 - 4x^2 + 3x - 1$ y que $b = 2$. Podemos usar las primeras tres hileras del siguiente esquema para encontrar

$$q_1(x) = x^3 + x^2 - 2x - 1$$

y $a_0 = -3$. Luego podemos continuar con el mismo esquema por dos hileras más para encontrar $q_2(x) = x^2 + 3x + 4$ y $a_1 = 7$. Análogamente, $q_3(x) = x + 5$, y $a_2 = 14$; $q_4(x) = 1$ y $a_3 = 7$; $a_4 = 1$.

					| 2
1	−1	−4	3	−1	
0	2	2	−4	−2	
1	1	−2	−1	−3	
0	2	6	8		
1	3	4	7		
0	2	10			
1	5	14			
0	2				
1	7				
0					
1					

En general, podemos escribir cualquier polinomio $p(x)$ de grado m como $q(x - b)$ y emplear la división sintética $(m + 1)$ veces para encontrar los coeficientes del nuevo polinomio $q(x - b)$. Es así como la teoría del Cap. III - 8 puede ahora verificarse para cualquier polinomio dado $p(x)$ y para cualquier número dado b. Nótese que esta reducción de los ceros o cambio de variable se lleva a cabo sin hacer ninguna referencia a los valores de los ceros del polinomio.

EJERCICIOS

1. Hacer el Ejercicio 1 del Cap. III-8, empleando el método anterior. Comparar este método con el que se utilizó en las Secciones 8 y 14 del Cap. III.
2. Hacer los Ejercicios 2 y 3 del Cap. III-8, empleando el método ya citado.
3. Escribir $x^5 - 7x^5 + x^4 - 3x^2 + 11$ en la forma $q(x - 2)$.
4. Escribir $x^7 - 1$ en la forma $q(x - 1)$.
5. Escribir $x^7 - 1$ en la forma $q(x + 1)$.
6. Encontrar las ecuaciones cuyas raíces son
a) dos menos que las de $x^3 - 7x^2 + 2x + 1 = 0$;
b) una más que las de $x^4 + 3x^3 - 5x^2 + x + 7 = 0$.

IV - 4 NUMERO DE RAICES. El aspecto más práctico de este capítulo es el que se refiere a cómo encontrar una o más raíces de una ecuación polinomia. En general, decimos que una ecuación polinomia está *resuelta* cuando se han determinado todas sus raíces. Por eso antes de resolver una ecuación polinomia es conveniente conocer el número total de raíces que se necesitan. Este número puede establecerse de antemano para cualquier polinomio dado con coeficientes complejos. Si el polinomio es una constante b, la ecuación no tiene raíces si $b \neq 0$, y tiene como raíces a todos los números complejos, si $b = 0$. Si el polinomio no es una constante, definiremos el grado de la ecuación polinomia $p(x) = 0$ como el mismo grado de $p(x)$ y obtendremos el

TEOREMA IV - 2 *Toda ecuación polinomia de grado $m > 0$ con coeficientes complejos tiene precisamente m raíces complejas (no necesariamente distintas).*

En la teoría de funciones de una variable compleja se demuestra fácilmente este teorema. No intentaremos dar aquí una de-

mostración completa, ya que ello implica, hasta cierto punto, demostraciones algebraicas. En cambio, daremos por aceptado el siguiente teorema y lo utilizaremos para demostrar el Teorema IV - 2.

TEOREMA IV-3. TEOREMA FUNDAMENTAL DEL ALGEBRA. *Todo polinomio $p(x)$ de grado positivo con coeficientes complejos tiene por lo menos un cero complejo.*

Los teoremas IV - 2 y IV - 3 están estrechamente relacionados con el hecho de que el conjunto de los números complejos es cerrado algebraicamente, como se señaló en la sección optativa Nº 18 del Capítulo I y que figura también como Ejercicio 6 en esa misma sección. Para el caso presente cualquier lector que omitió aquel ejercicio debería consultar otro texto o aceptar el Teorema IV - 3 sin una demostración rigurosa.

Ahora utilizaremos el Teorema IV-3 y demostraremos el Teorema IV - 2. Dado cualquier polinomio $p(x)$ de grado m, podemos, según el Teorema IV - 3, designar uno de sus ceros por el número complejo r_1 y de acuerdo con el Teorema IV - 1, escribir $p(x) = (x - r_1)p_1(x)$, en donde $p_1(x)$ es un polinomio de grado $m - 1$. Los coeficientes de $p_1(x)$ pueden encontrarse por división sintética y expresarse por medio del cero r_1, de los coeficientes de $p(x)$ y de las tres operaciones del anillo (Cap. IV - 2). Por lo tanto, los coeficientes de $p_1(x)$ son números complejos, y el procedimiento anterior puede repetirse para $p_1(x)$ si $m - 1 > 0$. Dado que el grado m de $f(x)$ es finito, este procedimiento puede repetirse sólo un número finito de veces, de donde resulta

$$\begin{aligned} p(x) &= (x - r_1)p_1(x), \\ p_1(x) &= (x - r_2)p_2(x), \\ p_2(x) &= (x - r_3)p_3(x), \\ &\cdot \\ &\cdot \\ &\cdot \\ p_{m-1}(x) &= (x - r_m)a_0, \end{aligned}$$

y

$$p(x) = a_0 (x - r_1)(x - r_2)(x - r_3) \ \ldots \ (x - r_m), \tag{IV-5}$$

en donde a_0 es el coeficiente inicial de $p(x)$.

El Teorema de Factorización Unica establece (Ejercicio 9, Cap.

III-6) que todo factor de $p(x)$ de la forma $x - b$ está contenido en (IV-5). Luego, el Teorema IV-1 establece que los ceros de $p(x)$ son precisamente $r_1, r_2, r_3, \ldots, r_m$. Esto completa la demostración del Teorema IV-2 mediante el Teorema IV-3. En lo que queda de este capítulo nos dedicaremos principalmente a la determinación de las raíces de ecuaciones polinomias.

EJERCICIOS

Demostrar los siguientes enunciados:

1. Cualquiera ecuación polinomia de la forma $d_0x^m + d_1x^{m-1} + \cdots + d_m = 0$ que tiene más de m raíces distintas es idénticamente nula, es decir, $d_i = 0$ para $i = 0, 1, 2, \ldots, m$.

2. Si dos polinomios $p(x)$ y $q(x)$ de grado m son iguales para más que m valores distintos de x, los polinomios son idénticos.

3. Si dos ecuaciones polinomias de grado m tienen precisamente las mismas raíces, los polinomios son asociados (Cap. III-4). [Indicación: Considérese $f(x) + kg(x)$, en que k se elige de tal modo que los términos de grado m desaparezcan].

IV-5 DETERMINACION DE LAS RAICES. Hemos visto que toda ecuación polinomia de grado m con coeficientes complejos tiene exactamente m raíces complejas (no necesariamente distintas). Queda aún el problema práctico de encontrar las raíces de una ecuación polinomia dada $p(x) = 0$.

La ecuación general lineal es de la forma $ax + b = 0$, en donde $a \neq 0$. Tiene una raíz única $x = -b/a$. Toda ecuación lineal con coeficientes racionales tiene una raíz racional; toda ecuación lineal con coeficientes complejos (reales o imaginarios) tiene una raíz compleja.

La ecuación general cuadrática es de la forma $ax^2 + bx + c = 0$, en donde $a \neq 0$. Sus dos raíces pueden encontrarse completando el cuadrado del miembro de la izquierda, de la manera siguiente:

$$x^2 + \frac{b}{a}x = -\frac{c}{a},$$

$$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = \frac{b^2}{4a^2} - \frac{c}{a},$$

$$x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a},$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Las dos raíces de $ax^2 + bx + c = 0$, en donde $a \neq 0$, entonces son

$$(-b + \sqrt{b^2 - 4ac})/2a \quad \text{y} \quad (-b - \sqrt{b^2 - 4ac})/2a.$$

El número $b^2 - 4ac$ se denomina el *discriminante* de la ecuación cuadrática. Si se designa respectivamente las dos raíces por r_1 y r_2, se puede verificar fácilmente que ellas satisfacen las relaciones elementales de simetría de los polinomios (Cap. IV-7) $r_1 + r_2 = -b/a$; $r_1 r_2 = c/a$. Si los coeficientes son números reales, tenemos

TEOREMA IV-4. *Una ecuación cuadrática con coeficientes reales tiene dos raíces que son reales y desiguales, reales e iguales, o conjugadas imaginarias según que el discriminante sea positivo, cero o negativo.*

Las raíces de las ecuaciones cúbica general (Cap. IV-9) y de cuarto grado (Cap. IV-10) pueden expresarse por medio de los coeficientes, empleando las cuatro operaciones fundamentales y radicales. La ecuación general de grado m, $m > 4$, no puede resolverse por medio de los coeficientes, utilizando las cuatro operaciones fundamentales y los radicales. Este resultado negativo puede probarse gracias a la obra de Evariste Galois en la teoría de los grupos. Lillian Lieber ha escrito un folleto muy interesante y ameno (Bibliografía Nº 32) donde señala este resultado y otras aplicaciones de las teorías de Galois.

El valor aproximado o la posición gráfica de los ceros reales de un polinomio $p(x)$ suele determinarse gracias a la continuidad de $p(x)$. Según el Ejercicio 4, Cap. III-13, todo polinomio en la variable real continua x es continuo para todos los valores finitos de x. Por eso (Ejercicio 5, Cap. III-13), si existen números reales a y b, $a < b$, tales que $p(a) \cdot p(b) < 0$, existe un número real c, $a < c < b$, tal que $p(c) = 0$. Además, puesto que $p(x)$ tiene el signo de su coeficiente inicial (Cap. III-1) para valores positivos de x suficientemente grandes, toda ecuación polinomia real de grado impar y coeficiente inicial positivo tiene, por lo menos, una raíz real de signo opuesto a su último término; toda ecuación polinomia real de grado par cuyo coeficiente inicial y término constante tengan signos opuestos, tiene, por lo menos, una raíz positiva y, por lo menos, una raíz negativa.

Consideraremos otros métodos en la Sección 14 de este Cap. IV, pero examinaremos primero, algo más, algunas de las relaciones entre los coeficientes y las raíces.

EJERCICIOS

Describir las raíces de las ecuaciones de los Ejercicios 1 a 7:

1. $5x - 17 = 0$.
2. $ix + 7i + 5 = 0$
3. $x^2 - 3x + 7 = 0$
4. $2x^5 - 7x + 35 = 0$
5. $x^4 - 3x^2 + 3x - 1 = (x - 1)^3$.
6. $5x^3 - 3x - 2 = 0$
7. $x^2 + 2x + 7 = x(x + 2)$.

8. Formar una ecuación cuadrática con raíces cuya suma es 3 y cuyo producto es 5. ¿Hay una respuesta única?

9. Encontrar la suma y el producto de las raíces de cada una de las siguientes ecuaciones:

a) $x^2 - 5x + 6 = 0$
b) $2x^2 - 3x + 5 = 0$
c) $3x^2 + 4x - 7 = 0$.

10. Describir (sin calcularlas) las raíces de las ecuaciones del Ejercicio 9.

IV-6 RAICES IMAGINARIAS CONJUGADAS.

Demostraremos el siguiente teorema:

TEOREMA IV-5. *Las raíces imaginarias de una ecuación polinomia con coeficientes reales se presentan en pares.*

Sea $p(z)$ un polinomio con coeficientes reales y supongamos que $p(w) = 0$, en que $w = a + bi$; a, b sean reales; $b \neq 0$. Demostraremos que $p(\bar{w}) = 0$ en donde $\bar{w} = a - bi$. El polinomio cuadrático

$$(z - w)(z - \bar{w}) = z^2 - 2az + a^2 + b^2$$

puede usarse con $p(z)$ en el Algoritmo de la División (Cap. III-5) para obtener:

$$p(z) = [z^2 - 2az + a^2 + b^2] \cdot g(z) + sz + t$$

en donde $g(z)$ es un polinomio. En $z = w$ tenemos $p(w) = 0 = 0 + sw + t$ o, por medio de $w = a + bi$, $0 = sa + sbi + t$. Igua-

lando las partes real e imaginaria de esta ecuación resulta $sa + t = 0$ y $sb = 0$, de donde $s = 0$ y $t = 0$, dado que $b \neq 0$. Luego $p(z) = (z - w)(z - \bar{w}) \cdot g(z)$; $p(\bar{w}) = 0$, y queda demostrado completamente el Teorema IV-5.

En el Cap. IV-4 vimos que todo polinomio $p(x)$ de grado m con coeficientes complejos tiene m raíces complejas. Esto implica que $p(x)$ podría escribirse como un producto de m factores lineales con coeficientes complejos (IV-5). En otras palabras, todo polinomio irreducible cuyos factores puedan tener coeficientes complejos arbitrarios, es lineal. El Teorema IV-5 y el hecho de que $(z - w)(z - \bar{w})$ sea un polinomio cuadrático con coeficientes reales implica ahora que todo polinomio irreductible cuyos factores puedan tener coeficientes reales arbitrarios es cuadrático o lineal. Un polinomio de cualquier grado m puede ser irreductible cuando los factores tienen coeficientes enteros o racionales. Por ejemplo, $x^m - 2$ para cualquier entero positivo m no tiene factores de grado menor que m con coeficientes racionales.

La solución de una ecuación polinomia y la factorización del polinomio en factores irreducibles son, por lo tanto, equivalentes, en el sentido del Teorema IV-1, sólo cuando los coeficientes de los factores pueden ser números complejos arbitrarios. En realidad, el conjunto de números complejos algebraicos es suficiente, como se señaló en el Cap. I-18.

EJERCICIOS

1. Demostrar que las raíces cuadráticas irracionales $a + \sqrt{b}$ de una ecuación polinomía con coeficientes racionales se presentan en pares conjugados.

2. Formar una ecuación racional cúbica, dadas dos de sus raíces: 1 y $3 - 2\sqrt{-1}$.

3. Formar una ecuación real de cuarto grado dadas dos de sus raíces: $1 + 5\sqrt{-1}$ y $5 - \sqrt{-1}$.

4. Dada la raíz $x = \sqrt{2}$ de $x^4 - 3x^3 - 2x + 6 = 0$, encontrar las otras dos raíces.

5. Dada la raíz $i/\sqrt{2}$ de $2z^4 - 12z^3 + 19z^2 - 6z + 9 = 0$, encontrar las otras tres raíces.

IV-7 POLINOMIOS ELEMENTALES SIMETRICOS. Hemos visto que cualquiera ecuación cuadrática $ax^2 + bx + c = 0$ tiene dos raíces r, s que satisfacen

las relaciones $r + s = -b/a$; $rs = c/a$ (Cap. IV-5). En general, si $p(x)$ es un polinomio de grado m con coeficientes complejos: los polinomios en los ceros de $p(x)$ que resultan de sumar todos los ceros de $p(x)$; la suma de todos los productos de pares de ceros de $p(x)$; la suma de todos los productos de triples de ceros de $p(x)$; . . .; el producto de todos los ceros de $p(x)$, pueden expresarse racionalmente por medio de los coeficientes de $p(x)$. Estos polinomios en los ceros de un polinomio $p(x)$ se denominan *polinomios elementales simétricos*.

Dado que pueden considerarse como ceros de un polinomio de grado m, a m números cualesquiera, podemos examinar los polinomios simétricos elementales de m números dados cualesquiera. Por ejemplo, los números 1, 2, 3 son ceros del polinomio $p(x) = (x - 1)(x - 2)(x - 3) = x^3 - 6x^2 + 11x - 6$. Los polinomios elementales simétricos de estos números o de los ceros de $p(x)$ pueden expresarse por medio de los coeficientes de $p(x)$ como sigue: $1 + 2 + 3 = 6$, el coeficiente de x^2 con el signo contrario; $1 \cdot 2 + 1 \cdot 3 + 2 \cdot 3 = 11$, o sea, el coeficiente de x; y $1 \cdot 2 \cdot 3 = 6$, o sea, el término constante de $p(x)$ con el signo contrario. En general, cuando el conjunto de coeficientes posibles forma un campo, podemos dividir cualquier polinomio $p(x)$ de grado m por su coeficiente inicial para obtener un polinomio primitivo que tiene los mismos ceros que $p(x)$. En el polinomio primitivo la suma de los m ceros es igual al coeficiente de x^{m-1} con el signo contrario; la suma de los productos de los ceros en pares es igual al coeficiente de x^{m-2}; . . .; el producto de los ceros es igual al término constante multiplicado por $(-1)^m$.

Estos resultados generales pueden obtenerse por medio del desarrollo (IV-5) de $p(x)$:

$$p(x) = a_0(x - r_1)(x - r_2)(x - r_3) \cdots (x - r_m).$$

Luego:

$$\begin{aligned} p(x) &= a_0[x^m - (r_1 + r_2 + \cdots + r_m)x^{m-1} \\ &\quad + (r_1r_2 + r_1r_3 + r_2r_3 + \cdots + r_{m-1}r_m)x^{m-2} - \cdots \\ &\quad + (-1)^m r_1r_2 \ldots r_m] \\ &= a_0[x^m - S_1x^{m-1} + S_2x^{m-2} - S_3x^{m-3} + \cdots + (-1)^m S_m], \end{aligned}$$

en donde S_j es el polinomio elemental simétrico de grado j, es decir,

$$S_1 = r_1 + r_2 + \ldots + r_m = \Sigma r_i,$$
$$S_2 = r_1r_2 + r_1r_3 + r_2r_3 + r_1r_4 + \ldots + r_{m-1}r_m = \Sigma r_ir_j,$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$S_j = \Sigma r_{i1}r_{i2} \ldots r_{ij},$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$S_m = r_1r_2r_3 \ldots r_m.$$

Dado un polinomio cualquiera de grado m, podemos obtener un polinomio primitivo correspondiente en el que la suma de los ceros es igual al coeficiente de x^{m-1} con el signo contrario; el producto de los ceros es $(-1)^m$ veces el término constante; y, en general, S_k es $(-1)^k$ veces el coeficiente de x^{m-k}. Por ejemplo, si $p(x) = (x + 1)(x - 1)(x + 2)(x - 2)$ con raíces -1, 1, -2, 2, entonces $p(x) = x^4 - 5x^2 + 4$, en donde el coeficiente principal es la unidad, el coeficiente de x^3 es $0 = -[(-1) + 1 + (-2) + 2]$, el coeficiente de x^2 es:
$-5 = (-1) \cdot 1 + (-1)(-2) + (-1) \cdot 2 + 1 \cdot (-2) + 1 \cdot 2 + (-2) \cdot 2$; el coeficiente de x es:
$0 = -[(-1) \cdot 1 \cdot (-2) + (-1) \cdot 1 \cdot 2 + (-1)(-2) \cdot 2 + 1 \cdot (-2) \cdot 2]$ y el término constante es $4 = (-1) \cdot 1 \cdot (-2) \cdot 2$.

Los polinomios elementales simétricos S_j pueden utilizarse para resolver ecuaciones polinomias cuando se conoce alguna relación adicional entre las raíces. Por ejemplo, si se conoce que dos de las raíces de la ecuación $x^3 - 4x^2 + 5x - 2 = 0$ son iguales, entonces las tres raíces pueden representarse por r, r, y s. Los polinomios elementales simétricos se aprovechan, en seguida, para completar la solución de la ecuación. Utilizando S_1 y S_2, tenemos $2r + s = 4$ y $2rs + r^2 = 5$. Estas dos ecuaciones pueden resolverse simultáneamente sustituyendo en la cuadrática, un valor de la lineal y resulta $2r(4 - 2r) + r^2 = 5$; $3r^2 - 8r + 5 = 0$, de donde $r = 1$ y $s = 2$; o bien $r = \frac{5}{3}$ y $s = \frac{2}{3}$ El segundo par de valores no proporciona el valor correcto para S_3 ya que debemos obtener $r^2s = 2$, y por eso la ecuación dada tiene las raíces 1, 2, y 2.

Cuando no se sabe nada sobre las raíces de una ecuación polinomia, excepto que son raíces de $p(x) = 0$, el empleo de polinomios elementales simétricos conduce meramente a otra ecuación

que es esencialmente equivalente a $p(x) = 0$. Por ejemplo, supongamos que $x^2 + bx + c = 0$ tiene raíces r y s. Entonces $r + s = -b$; $rs = c$, y, por sustitución, $r(-b-r) = c$, o bien $r^2 + br + c = 0$.

Los siguientes ejercicios comprenden varias aplicaciones de los resultados anteriores. En la sección siguiente de este capítulo, consideraremos otras aplicaciones importantes de los polinomios elementales simétricos.

EJERCICIOS

1. Sin valerse de factores lineales, encontrar:
   a) una ecuación cúbica que tenga las raíces 1, 2, 3;
   b) una ecuación cúbica que tenga las raíces 0, −2, 2;
   c) una ecuación de cuarto grado que tenga las raíces 2, 2, −2, −2.

2. Dado $x^4 + 14x^3 + 73x^2 + 168x + 144 = 0$, que tiene dos raíces dobles, encontrar las raíces.

3. Dado $x^3 - 27x^2 + 242x - 720 = 0$, que tiene una raíz igual a la mitad de la suma de las otras dos, encontrar las raíces.

4. Dado $x^3 + 7x^2 - 6x - 72 = 0$, que tiene dos raíces en la razón de 3 es a 2, encontrar las tres raíces.

5. Si una de las raíces de las ecuaciones siguientes es la negativa de la otra, resolver:
   a) $4x^3 - 12x^2 - 25x + 75 = 0$;
   b) $4x^3 - 16x^2 - 9x + 36 = 0$.

6. ¿Qué relaciones deben existir entre los coeficientes de una ecuación general de segundo grado si una raíz es el doble de la otra?

7. Resolver $x^3 + 7x^2 - 21x - 27 = 0$, si se sabe que sus raíces están en progresión geométrica.

8. Resolver $x^3 - 3x^2 - 13x + 15 = 0$, si se sabe que sus raíces están en progresión aritmética.

IV-8 TRANSFORMACIONES DE RAICES. Esta sección es, principalmente, una ampliación de las secciones Cap. III - 8 y Cap. IV - 3. En Cap. III - 8 encontramos que cualquier polinomio $p(x)$ podía expresarse teóricamente en la forma $q(ax + b)$, en donde $a \neq 0$. En el Cap. IV-3 empleamos la división sintética para obtener el nuevo polinomio en el caso especial de que $a = 1$. En esta parte del Cap. IV nos valdremos de los polinomios elementales simétricos para obtener el nuevo polinomio $q(ax + b)$ para cualquier $a \neq 0$, es decir, dado un polinomio $p(x)$ con ceros r_j $(j = 1, 2, \ldots, m)$ encontraremos un polinomio $q(y)$ con ceros $ar_j + b$ para números cualesquiera $a \neq 0$ y b.

Cualquier polinomio con coeficientes pertenecientes a un campo y ceros $r_1, r_2, \ldots, r_m$ tiene un polinomio asociado de la forma $p(x) = x^m - S_1x^{m-1} + S_2x^{m-2} + \ldots + (-1)^jS_jx^{m-j} + \ldots + (-1)^mS_m$, en que los S_j son los polinomios elementales simétricos de grado j (Cap. IV-7). Si multiplicamos cada r_j por un número k, entonces

$$kr_1 + kr_2 + \cdots + kr_m = k(r_1 + r_2 + \cdots + r_m) = kS_1,$$
$$(kr_1)(kr_2) + (kr_1)(kr_3) + (kr_2)(kr_3) + \cdots + (kr_{m-1})(kr_m) = k^2S_2,$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$(kr_1)(kr_2)(kr_3)\ldots(kr_m) = k^mS_m.$$

Es así como la multiplicación de los ceros de $p(x)$ por k da como resultado la multiplicación del polinomio elemental simétrico S_j por k^j. A la inversa, si multiplicamos S_j por k^j obtenemos un nuevo polinomio que tiene exactamente tantos ceros como sean k veces los ceros de $p(x)$. Por ejemplo, $x^2 - 4x + 3$ tiene los ceros 1 y 3, en que $S_1 = 4$ y $S_2 = 3$. Si formamos un nuevo polinomio, valiéndonos de $2S_1 = 8$ y $2^2S_2 = 12$ como los nuevos polinomios simétricos elementales, obtenemos $q(y) = y^2 - 8y + 12$ con ceros 2 y 6. En general, tenemos,

TEOREMA IV-6. *Dado un polinomio* $p(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m$ *y un número* k, *podemos inmediatamente escribir un polinomio* $q(y) = a_0y^m + a_1ky^{m-1} + a_2k^2y^{m-2} + \ldots + a_mk^m$ *con tantos ceros como sea el producto de* k *por los ceros de* $p(x)$.

En el Teorema siguiente, IV-7, discutiremos un procedimiento para obtener un polinomio con ceros que sean los recíprocos de los ceros de un polinomio dado. Por ejemplo, dado el polinomio $x^2 - x - 6$ con ceros 3 y -2, podemos, según el Teorema IV-7, obtener $1 - x - 6x^2$ con ceros $\frac{1}{3}$ y $-\frac{1}{2}$. En relación con este teorema es necesario tener en cuenta que un polinomio adquiere una raíz infinita (que se designa por $a/0$ en donde $a \neq 0$) cada vez que su coeficiente principal se hace cero. Esta convención es consistente con el resultado obtenido por medio de los límites (Cap. III-11), dado que, por lo menos, un cero de $p(x)$ crece indefinidamente a medida que el coeficiente principal de $p(x)$ tiende a cero. Según la convención anterior para las raíces infinitas, resulta:

TEOREMA IV-7. *Dado un polinomio* $p(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m$, *podemos inmediatamente escribir un polinomio* $h(u) = a_0 + a_1u + a_2u^2 + \ldots + a_mu^m$ *cuyos ceros son los recíprocos de los ceros de* $p(x)$.

El asunto de las raíces infinitas del que hemos hablado anteriormente surge, por ejemplo, cuando hacemos $p(x) = x^2 - x$ con raíces 1 y 0 aplicamos el teorema anterior para obtener $h(u) = 0 \cdot u^2 - u + 1$ cuyos ceros son 1 y $\frac{1}{0}$. La demostración del Teorema IV-7, la dejaremos como ejercicio (Ejercicio 6).

Después de esto, podemos efectuar tres transformaciones en los ceros de cualquier polinomio dado $p(x)$ con ceros $r_1, r_2, \ldots, r_m$. Podemos encontrar $f(v)$ con ceros $r_j - b$ (Cap. IV-3); $q(y)$ con ceros ar_j $(a \neq 0)$ (Teorema IV-6); y $h(u)$ con ceros $1/r_j$ (Teorema IV-7). Estas tres transformaciones son suficientes para demostrar el siguiente teorema:

TEOREMA IV-8. *Dado un polinomio* $p(x)$ *con coeficientes complejos y ceros* r_j $(j = 1, 2, \ldots, m)$, *podemos obtener un polinomio* $q(y)$ *con ceros* $s_j = (ar_j + b)/(cr_j + d)$ $(j = 1, 2, \ldots, m)$ *en que* a, b, c, d *sean números complejos cualesquiera tales que* $ad - bc \neq 0$, *por medio de únicamente los coeficientes de* $p(x)$ *y las cuatro operaciones fundamentales.*

La condición $ad - bc \neq 0$, hace posible expresar r_j (Ejercicio 7, Cap. III-10) racionalmente en función de s_j, $r_j = (a's_j + b')/(c's_j + d')$, es decir efectuar cualquiera transformación lineal biracional en los ceros de un polinomio dado $p(x)$.

Dividiremos la demostración del Teorema IV-8 en dos casos. Si $c = 0$, utilizaremos las dos transformaciones sucesivas $t_1 = ax/d$; $y = t_1 + b/d$. Si $c \neq 0$, usaremos las cinco transformaciones $t_1 = cx$;

$$t_2 = t_1 + d = cx + d; \qquad t_3 = 1/t_2 = 1/(cx + d);$$
$$t_4 = (b - ad/c)t_3 = (bc - ad)/[c(cx + d)];$$

$y = t_4 + a/c = (ax + b)/(cx + d)$. Dado que cada una de estas transformaciones es alguna de las tres formas que podemos efectuar, queda, pues, demostrado completamente el Teorema IV - 8.

Una de las aplicaciones más útiles de los polinomios elementales simétricos se expresa en el siguiente teorema, que demostra-

remos por medio de transformaciones de las raíces, de una ecuación polinomia.

TEOREMA IV-9. *Toda raíz racional de una ecuación polinomia* $a_0x^m + a_1x^{m-1} + a_2x^{m-2} \ldots + a_m = 0$ *con coeficientes enteros, puede expresarse en la forma* b_m/b_0, *en que* $(b_m, b_0) = 1$, b_m *es divisor de* a_m *y* b_0 *es divisor de* a_0.

Este teorema se presta para encontrar todas las raíces racionales de cualquiera ecuación polinomia dada con coeficientes enteros en un número finito de etapas. Nos permite emplear cuando más la fórmula cuadrática para resolver completamente cualquiera ecuación polinomia con coeficientes enteros y que tengan a lo sumo dos raíces no racionales. Por ejemplo, las únicas raíces racionales posibles de $x^3 - x^2 + x - 1 = 0$ son 1 y -1. Estas pueden comprobarse por sustitución o por división sintética. En seguida, la ecuación polinomia dada puede expresarse como $(x - 1)(x^2 + 1) = 0$, de donde sus raíces son 1, i, $-i$.

Tal como se señaló anteriormente, el Teorema IV-9, puede demostrarse por medio de transformaciones de raíces. Supongamos que $p(x) = 0$ tenga una raíz racional b_m/b_0. Podemos suponer que $(b_m, b_0) = 1$. Si aplicamos el Teorema IV-6 y multiplicamos las raíces de $p(x) = 0$ por b_0, entonces S_m y $b_0^m a_m/a_0$ tienen el mismo valor numérico, la raíz b_m debe ser divisor de S_m y por lo tanto b_m debe ser divisor de $b_0^m a_m$. Puesto que $(b_m, b_0) = 1$, b_m es divisor de a_m según el Teorema II-9. Análogamente, b_0 es divisor de a_0, según el Teorema IV-7 (Ejercicio 10). Dado que cualquier polinomio con coeficientes racionales tiene un polinomio asociado con coeficientes enteros, el Teorema IV-9 puede también utilizarse para encontrar todas las raíces racionales de cualquiera ecuación polinomia con coeficientes racionales.

Los polinomios elementales simétricos tienen una considerable importancia teórica, aparte de las aplicaciones citadas en las transformaciones de los ceros de los polinomios y en la solución de ecuaciones polinomias con coeficientes racionales. Los polinomios elementales simétricos en las raíces de una ecuación polinomia pueden siempre expresarse racionalmente por medio de los coeficientes del polinomio original.

Se dice que un polinomio $p(r_1, r_2, \ldots, r_n)$ es simétrico si permanece invariable al efectuar todos los cambios posible de r_i y r_i. Por ejemplo, $x + y$; xy; $x^2 + y^2$; $xy - x - y$; y $x^3 - xy + y^3 - 2$

son polinomios simétricos en x e y. Se puede probar (ver Bibliografía Nº 49; pág. 264) que todo polinomio simétrico en los ceros de un polinomio $p(x)$ es un polinomio en los polinomios elementales simétricos y por lo tanto puede expresarse racionalmente por medio de los coeficientes de $p(x)$. Ejemplos de esta propiedad son los Ejercicios 14 y 15.

El tema de los polinomios simétricos o funciones simétricas se encuentra tratado extensamente en muchos textos sobre teoría de las ecuaciones. Concluiremos nuestra breve discusión de esta materia con los ejercicios que siguen. En las dos secciones siguientes, que son optativas, volveremos al problema de resolver ecuaciones y en particular a la resolución de ecuaciones cúbicas y de cuarto grado. Después de eso examinaremos métodos para determinar el número de raíces reales de una ecuación polinomia.

EJERCICIOS

1. Dado $x^3 - 2x^2 - 5x + 6 = 0$ con raíces 1, —2, 3, encontrar una ecuación polinomia con raíces —1, 2, —3.

2. Generalizar el método empleado en el Ejercicio 1 y proponer un procedimiento para encontrar una ecuación polinomia $q(y) = 0$ con raíces $-r_j$ correspondientes a cualquier $p(x) = 0$ dado con raíces r_j.

3. Dado un polinomio $p(x)$, demostrar el Teorema IV-6, resolviendo la relación $y = kx$ para x y sustituyendo este valor en $p(x)$.

4. Encontrar un polinomio $q(y)$, cuyos ceros sean iguales a tres veces los ceros de

$$p(x) = x^3 - 3x^2 + 2x - 1 .$$

Escríbase primero la respuesta de acuerdo con el Teorema IV-6 y en seguida compruébese esta respuesta por el método dado en el Ejercicio 3.

5. Encontrar un polinomio $q(y)$, cuyos ceros sean —2 veces los ceros de $p(x) = x^4 + 2x^3 - x^2 + x + 1$.

Emplear el mismo procedimiento que en el Ejercicio 4.

6. Demostrar el Teorema IV-7, por medio de polinomios simétricos.

7. Formular de nuevo y transformar el Ejercicio 3, según el Teorema IV-7.

8. Escribir un polinomio con ceros que sean los recíprocos de los ceros del polinomio $p(x)$ dado en el Ejercicio 5. Comprobar esta respuesta por el método dado en el Ejercicio 7.

9. Formular de nuevo y transformar el Ejercicio 3, según el Teorema IV-8

10. Demostrar que b_n es divisor de a_0 en el Teorema IV-9.

11. Encontrar las raíces racionales, y luego resolver completamente:

a) $2y^3 - y^2 - 4y + 2 = 0$;

b) $2x^4 - 12x^3 + 19x^2 - 6x + 9 = 0$.

12. Encontrar todas las raíces racionales de:

a) $3y^4 - 40y^3 + 130y^2 - 120y + 27 = 0$;

b) $3y^3 - 2y^2 + 9y - 6 = 0$;

c) $108y^3 - 270y^2 - 42y + 1 = 0$;

d) $24y^3 - 2y^2 - 5y + 1 = 0$.

13. Encontrar las raíces enteras de las ecuaciones:

(a) $x^4 + 6x^3 + x^2 - 24x - 20 = 0$;

(b) $x^4 + 11x^3 + 41x^2 + 61x + 30 = 0$.

14. Dada una ecuación cúbica $x^3 + ax^2 + bx + c = 0$, con raíces, r, s, t, encontrar una fórmula para la función simétrica $r^2 + s^2 + t^2$ por medio de los coeficientes de la ecuación dada. Escribir nuevamente esta fórmula valiéndose de los polinomios elementales simétricos S_1, S_2, y S_3.

15. Dada una ecuación cuadrática $x^2 + px + q = 0$ con raíces r y s, expresar los polinomios simétricos siguientes como polinomios en los polinomios elementales simétricos:

a) $r^2 + s^2$;

b) $r - rs + s$;

c) $r^2 - rs + s^2 - 2$;

d) $r(r^2 + s - r) + s(s^2 + r - s)$.

*IV.-9 ECUACIONES CUBICAS. En el Cap. IV-5 dejamos establecido que las ecuaciones generales polinomias de grado 1, 2, 3 y 4 podían resolverse por medio de las cuatro operaciones fundamentales (adición, sustracción, multiplicación y división) y de los radicales. En el Cap. IV-5 se trataron las ecuaciones lineales y cuadráticas; las ecuaciones cúbicas se tratarán en esta sección; y las ecuaciones de cuarto grado en la sección siguiente. Como se hacía notar en el Cap. IV-5, no existe ningún método análogo para resolver ecuaciones generales de grado mayor que cuatro. Podemos resolver cualquier ecuación polinomia dada con coeficientes enteros que tenga a lo sumo cuatro raíces no racionales, cualquiera que sea el grado de la ecuación (Cap. IV-8). También podemos resolver ciertas ecuaciones de grado mayor que cuatro (Cap. IV-13). Sin embargo, aún no podemos resolver por medio de un número finito de operaciones racionales y de radicales una ecuación general $a_0x^m + a_1x^{m-1} + \ldots + a_m = 0$ en que m sea mayor que cuatro.

Basaremos nuestro método de resolver ecuaciones cúbicas y de cuarto grado sobre las transformaciones de las raíces (Cap. IV-8). Ensayemos primeramente este método en la ecuación cuadrática general. La ecuación cuadrática general $ax^2 + bx + c = 0$, $a \neq 0$ con raíces r_1, r_2, pudo haberse resuelto haciendo dos transforma-

ciones en las raíces r_1, r_2. La ecuación $g(y) = y^2 + 2by + 4ac = 0$ tiene raíces $2ar_j$, según el Teorema IV - 6. Esto es análogo a la derivación previa de las raíces, pues el coeficiente inicial es ahora 1, y nos disponemos en seguida a dividir el coeficiente del término lineal por 2. Dado que la suma de las raíces de $g(y)$ es $-2b$, disminuimos las raíces en $-b$ para obtener una nueva ecuación sin término lineal, que por este motivo pueda resolverse factorizándose como la diferencia de dos cuadrados. La nueva ecuación puede determinarse por división sintética (Cap. IV - 3).

			$\lfloor -b$
1	$2b$	$4ac$	
0	$-b$	$-b^2$	
1	b	$4ac - b^2$	
0	$-b$		
1	0		
0			
1			

y resulta $x^2 + (4ac - b^2) = 0$ con raíces s_1, s_2, en que $s_j = 2ar_j + b$. Luego $s_j = \pm\sqrt{b^2 - 4ac}$ y la relación $r_j = (s_j - b)/2a$ proporciona las raíces r_j en la forma acostumbrada. Se puede utilizar un procedimiento análogo para facilitar la resolución de ecuaciones cúbicas y de cuarto grado.

Sea la ecuación general cúbica

$$p(x) = ax^3 + bx^2 + cx + d = 0, \quad a \neq 0$$

y sean r_1, r_2, r_3, sus raíces. Para obtener el coeficiente inicial 1 y para que la suma de las raíces sea fácilmente divisible por 3, aplicamos el Teorema IV - 6 para obtener, después de dividir por a,

$$g(y) = y^3 + 3by^2 + 9acy + 27a^2d = 0$$

con raíces $3ar_j$. Como anteriormente, disminuimos las raíces en $-b$, por medio de la división sintética,

				$\lfloor -b$
1	$3b$	$9ac$	$27a^2d$	
0	$-b$	$-2b^2$	$2b^3 - 9abc$	
1	$2b$	$9ac - 2b^2$	$2b^3 - 9abc + 27a^2d$	
0	$-b$	$-b^2$		
1	b	$9ac - 3b^2$		
0	$-b$			
1	0			
0				
1				

para obtener

$$h(z) = z^3 + (9ac - 3b^2)z + (2b^3 - 9abc + 27a^2d) = 0.$$

Esta ecuación se llama *cúbica reducida*. La escribiremos nuevamente en la forma

$$z^3 + pz + q = 0,$$

en donde $p = 9ac - 3b^2$ y $q = 2b^3 - 9abc + 27a^2d$.

Hay dos procedimientos muy conocidos para continuar con la resolución de la ecuación cúbica. Podemos reducir el problema a una forma más sencilla mediante una nueva transformación $z = t - p/3t$ (Bibliografía Nº 47; pág. 105); o bien podemos simplificarla de otra manera por medio de la sustitución $z = u + v$ (Bibliografía Nº 49; pág. 85). Consideremos el segundo método. Reemplazamos la única variable z por dos variables u, v. Puede ser necesario que estas dos variables satisfagan otra condición que elegiremos dentro de poco. Por medio de la sustitución, la ecuación cúbica reducida, tiene la forma

$$u^3 + v^3 + (3uv + p)(u + b) + q = 0.$$

Elegiremos ahora $3uv + p = 0$ como la nueva condición para las nuevas variables u, v, de modo que la ecuación anterior tenga la forma

$$u^3 + v^3 + q = 0$$

Luego la resolución de la ecuación cúbica reducida es equivalente a la resolución simultánea de $u^3 + v^3 = -q$ y $uv = -p/3$. El cubo de la última ecuación es $u^3v^3 = -p^3/27$. De este modo u^3 y v^3 son dos variables cuya suma es $-q$ y cuyo producto es $-p^3/27$, es decir, son las dos raíces de

(IV - 6) $$t^2 + qt - p^3/27 = 0.$$

Por lo tanto, podemos elegir

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = A,$$

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = B.$$

Los valores posibles de u son $\sqrt[3]{A}$, $\omega\sqrt[3]{A}$, $\omega^2\sqrt[3]{A}$, y los valores de v son $\sqrt[3]{B}$, $\omega\sqrt[3]{B}$, $\omega^2\sqrt[3]{B}$, , en que ω es una raíz cúbica primi-

tiva de la unidad (Cap. I - 17). Ya que por hipótesis $uv = -p/3$, estos valores deben asociarse en pares como sigue:

$$\begin{aligned} u_1 &= \sqrt[3]{A}, & v_1 &= \sqrt[3]{B}, \\ u_2 &= \omega\sqrt[3]{A}, & v_2 &= \omega^2\sqrt[3]{B}, \\ u_3 &= \omega^2\sqrt[3]{A}, & v_3 &= \omega\sqrt[3]{B}. \end{aligned}$$

Luego, volviendo atrás, vemos que las raíces r_j de la ecuación original deben estar dadas por $r_j = (u_j + v_j - b)/3a$ $(j = 1, 2, 3)$. Estas fórmulas para las raíces de una ecuación cúbica se conocen como las *fórmulas de Cardán*.

Es así como hemos empleado números complejos y radicales para expresar las raíces de una ecuación cúbica general por medio de sus coeficientes. La ecuación cúbica tiene una raíz real y dos conjugadas imaginarias, si (IV - 6) tiene raíces reales distintas; tiene tres raíces reales de las cuales por lo menos dos son iguales si (IV - 6) tiene raíces iguales; tiene tres raíces reales distintas si (IV - 6) tiene raíces imaginarias. En la mayoría de los textos sobre teoría de las ecuaciones se estudian estos casos y los métodos especiales para proceder en los diversos tipos de ecuaciones cúbicas. En particular, cuando la ecuación cúbica tiene coeficientes reales y tres raíces reales distintas, suele ser conveniente expresar las raíces como funciones reales de los coeficientes por medio de funciones trigonométricas. Este método es especialmente útil si la ecuación cúbica tiene coeficientes racionales y tres raíces irracionales, ya que en este caso (Bibliografía Nº 49; págs. 91-92) no es posible expresar ninguna raíz por medio de radicales reales y no es posible obtener las raíces por medio de las fórmulas de Cardán empleando operaciones racionales.

Apliquemos la teoría citada a una ecuación cúbica, por ejemplo, $x^3 - x^2 + x - 1 = 0$, que podamos también resolver por los métodos del Cap. IV - 8. Esta ecuación tiene las raíces 1, i, $-i$. Por eso, el uso de las fórmulas de Cardán aquí se convierte simplemente en una ilustración del método para esta ecuación cúbica particular. Primero multiplicamos las raíces por $3a = 3$ y obtenemos $g(y) = y^3 - 3y^2 + 9y - 27 = 0$. En seguida disminuimos las raíces en $-b = 1$, por medio de la división sintética, y obtenemos $h(z) = z^3 + 6z - 20$. Hacemos, en seguida, $z = u + v$, en que $uv = -\frac{6}{3}$

$= -2$. Entonces, $u^3v^3 = -8$ y, por sustitución, en $h(z)$, $u^3 + v^3 = 20$. Estos polinomios elementales simétricos en u^3 y v^3 pueden usarse para formar una ecuación cuadrática $t^2 - 20t - 8 = 0$ que tiene como raíces u^3 y v^3. Dado que las raíces son $10 \pm 6\sqrt{3}$, podemos elegir $u^3 = 10 + 6\sqrt{3}$ y $v^3 = 10 - 6\sqrt{3}$. Gracias a este método sabemos ahora que la ecuación dada tiene una raíz real y dos raíces imaginarias conjugadas. Luego, por medio $\omega = (-1 + i\sqrt{3})/2$, se obtiene

$$u_1 = \sqrt[3]{10 + 6\sqrt{3}}, \qquad v_1 = \sqrt[3]{10 - 6\sqrt{3}},$$
$$u_2 = [(-1 + i\sqrt{3})\sqrt[3]{10 + 6\sqrt{3}}]/2, \qquad v_2 = [(-1 - i\sqrt{3})\sqrt[3]{10 - 6\sqrt{3}}]/2,$$
$$u_3 = [(-1 - i\sqrt{3})\sqrt[3]{10 + 6\sqrt{3}}]/2, \qquad v_3 = [(-1 + i\sqrt{3})\sqrt[3]{10 - 6\sqrt{3}}]/2.$$

Finalmente, por medio de $r_j = (u_j + v_j + 1)/3$ y muchas simplificaciones aritméticas, se obtiene $r_1 = 1$, $r_2 = i$, $r_3 = -i$. La ecuación cúbica en referencia, puede también resolverse tomando en cuenta raíces racionales. Las fórmulas de Cardán proporcionan el mismo resultado que los otros métodos, pero exigen más trabajo. Recurriremos a las fórmulas únicamente cuando los otros métodos no sirvan. Su importancia reside en que proporcionan un método seguro, aunque tedioso, para expresar las raíces de cualquiera ecuación cúbica con coeficientes complejos por medio de radicales.

EJERCICIOS

Resolver las siguientes ecuaciones:

1. $x^4 - 7x^2 + 15x - 9 = 0$
2. $x^3 + 2x + 20 = 0$
3. $x^3 - 3x^2 - 2x + 5 = 0$
4. $24y^3 - 2y^2 - 5y + 1 = 0$

*IV-10 ECUACIONES DE CUARTO GRADO. Ahora consideraremos la resolución de ecuaciones polinomias de cuarto grado. Como en el caso de las ecuaciones cúbicas, nuestro método se basará sobre transformaciones de las raíces. También como en el caso de las ecuaciones cúbicas, emplearemos este método sólo cuando no sea posible aplicar otros métodos, tales como encontrar las raíces racionales (Cap. IV-8) y encontrar las raíces múltiples (Cap. IV-13).

Sea la ecuación general de cuarto grado

$$f(x) = ax^4 + bx^3 + cx^2 + dx + e = 0, \qquad a \neq 0$$

y sean sus raíces r_j $(j = 1, 2, 3, 4)$. El primer método para resolver las ecuaciones de cuarto grado fue descubierto por Ferrari, un alumno de Cardán. Uspensky (Bibliografía Nº 49; págs. 94-97) presenta una discusión amena y completa del método de Ferrari. Nosotros usaremos el método de Descartes (Bibliografía Nº 47; págs. 114-117). Se multiplican primero las raíces por $4a$ y se divide la nueva ecuación por a para obtener

$$g(y) = y^4 + 4by^3 + 16acy^2 + 64a^2dy + 256a^3e = 0.$$

Luego se disminuyen las raíces en $-b$ y se obtiene una ecuación de la forma

$$z^4 + pz^2 + qz + r = 0 \qquad \text{(IV - 7)}$$

en donde p, q, r, son polinomios en los coeficientes de $f(x)$.

Dado que en el conjunto de polinomios con coeficientes reales todo polinomio irreducible es lineal o cuadrático (Cap. IV - 6), la ecuación (IV - 7) puede expresarse como el producto de dos polinomios cuadráticos. Si (IV - 7) tiene coeficientes reales, los nuevos polinomios tendrán coeficientes reales. Además, ya que la suma de las raíces de (IV - 7) es cero, la suma de las cuatro raíces de los factores cuadráticos debe ser cero y la suma de los factores cuadráticos separadamente debe ser la misma, excepto en el signo. Por consiguiente la ecuación (IV - 7) puede expresarse en la forma

$$(z^2 - kz + n)(z^2 + kz + m) = 0. \qquad \text{(IV - 8)}$$

Dado que los miembros de la izquierda de (IV - 7) y de (IV - 8) son idénticamente iguales, se tiene $n + m - k^2 = p$; $k(n - m) = q$; y $nm = r$.

A continuación se elimina n y m de estas ecuaciones. Se obtiene:

$$k^2(n + m)^2 = k^2(k^2 + p)^2,$$
$$k^2(n - m)^2 = q^2$$

y por sustracción se obtiene $4k^2nm = k^2(k^4 + 2k^2p + p^2) - q^2$, o

$$k^6 + 2pk^4 + (p^2 - 4r)k^2 - q^2 = 0,$$

o sea, la *resolvente cúbica* en k^2. La resolvente cúbica puede resolverse y sus raíces designarse por los números complejos $4A^2$, $4B^2$, $4C^2$. Entonces el producto de las raíces es $q^2 = 64\,A^2B^2C^2$, y podemos elegir A, B, C, tales que $q = -8ABC$. Análogamente, la suma de

las raíces $-2p = 4(A^4 + B^4 + C^4)$. Si alguna raíz de la resolvente cúbica es diferente de cero, supongamos $2A \neq 0$; en todo caso elegimos $k = 2A$. Luego, de $n + m - k^2 = p$, $p = -2(A^2 + B^2 + C^2)$, y $k^2 = 4A^2$, se obtiene

$$n + m = k^2 + p = 2(A^2 - B^2 - C^2).$$

Análogamente, de $k = 2A$; $q = -8ABC$, y $k(n - m) = q$, se obtiene

$$n - m = -4BC.$$

De estas dos relaciones en n y en m, resulta

$$n = (A + B + C)(A - B - C),$$
$$m = (-A + B - C)(-A - B + C).$$

En vista de que las sumas de los factores de n y m son, respectivamente, k y $-k$, estos cuatro factores son las raíces de (IV - 8) y por lo tanto de (IV - 7). Las raíces de la ecuación de cuarto grado dada se obtienen de las de (IV - 7) sumando $-b$ y dividiendo por $4a$. En consecuencia, las raíces de una ecuación de cuarto grado general pueden expresarse por medio de los coeficientes empleando radicales. Como se señaló en el Cap. IV - 5, este procedimiento no puede continuar más allá, puesto que una ecuación general de grado mayor que cuatro no puede resolverse por medio de las cuatro operaciones fundamentales y de los radicales.

EJERCICIOS

Resolver las siguientes ecuaciones:

1. $x^4 - 2x^3 - 3x^2 + 4x + 4 = 0$
2. $3x^4 - 3x^3 - 2x + 5 = 0$
3. $x^4 - x^3 + 10x - 4 = 0$
4. $x^4 - 6x^2 - 8x - 3 = 0$

IV-11 LA REGLA DE DESCARTES PARA LOS SIGNOS. Volvemos ahora a la tarea de determinar diversos tipos de raíces de ecuaciones polinomias. Cualquier polinomio de grado m con coeficientes complejos tiene m raíces complejas (Cap. IV - 4). Las raíces racionales de cualquier ecuación polinomia con coeficientes enteros (o racionales) pueden encontrarse después de un número finito de etapas (Cap. IV - 8). En esta sección consideraremos un método para calcular el número de raíces reales de cualquiera ecuación polinomia dada con coeficientes

reales. Para ser exactos, estimaremos el número de raíces positivas, determinaremos el número de raíces cero y estimaremos el número de raíces negativas. En la parte siguiente de este Capítulo, estudiaremos un método para determinar exactamente el número de raíces reales de una ecuación polinomia con coeficientes reales en cualquier intervalo (Cap. III - 10) de la forma $a < x \leqq b$. La importancia del método que presentamos en esta sección, reside en su sencillez.

Cuando todas las raíces de una ecuación polinomia $f(x) = 0$ son reales y positivas, todos los polinomios elementales simétricos son positivos y los coeficientes de $f(x)$ tienen signos alternados, puesto que

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \ldots + a_n$$
$$= a_0\,[x^n - S_1x^{n-1} + S_2x^{n-2} - S_3x^{n-3} + \ldots + (-1)^nS_n].$$

Por otra parte, todos los coeficientes de $f(x)$ tienen el mismo signo cuando todas las raíces son negativas. Buscaremos ahora relaciones más exactas entre los coeficientes de la ecuación $f(x) = 0$ y la ubicación de sus raíces.

Dos términos consecutivos de un polinomio real en el cual se han suprimido los términos con coeficientes cero se dice que presentan una *variación* o una *permanencia* de signo según que sus coeficientes tengan signos desiguales o iguales. Por ejemplo, $x^4 - 1$ tiene una variación y $x^2 + 1$ tiene una permanencia.

Consideremos un polinomio $f(x)$ y supongamos, por ejemplo, que no tiene coeficientes cero y que los signos de sus coeficientes están dados como en el cuadro (IV - 9) más adelante. En seguida calculamos los signos de $g(x) = (x - r)f(x)$, en que r es cualquier número positivo, e indicamos los signos de los coeficientes de $g(x)$ por $\pm$ todas las veces que los signos dependan de los valores de r y de los coeficientes de $f(x)$.

(IV - 9)

$f(x)$:	+	+	−	−	−	+	−	−	+	+	−	
$(x - r)$:	+	−										
	+	+	−	−	−	+	−	−	+	+	−	
		−	−	+	+	+	−	+	+	−	−	+
$g(x)$:	+	±	−	±	±	+	−	±	+	±	−	+

La sucesión de los coeficientes del polinomio $f(x)$ que se muestra más arriba tiene cinco variaciones de signo: la sucesión de los de

$g(x)$ tiene por lo menos seis variaciones y podría tener ocho, pero nunca siete.

En general, para cualquier polinomio $f(x)$ dado con coeficientes reales y cualquier número r positivo dado, puede probarse (Ver Bibliografía Nº 19; págs. 446-447) que la sucesión de coeficientes del polinomio $g(x) - (x - r)f(x)$ tiene por lo menos una variación más de signo que la sucesión correspondiente a $f(x)$. Esta proposición puede probarse por medio de las relaciones $c_0 = b_0$ y $c_j = b_j + c_{j-1}r$, en que los c_j son los coeficientes de $f(x)$ y los b_j son los coeficientes de $g(x)$ (Cap. IV - 2). Por ejemplo, si la sucesión $b_0, b_1, \ldots, b_n$, no contiene ninguna variación, entonces la sucesión $c_0, c_1, \ldots, c_n$, no contiene ninguna variación. Si, además, la sucesión $b_v, \ldots, b_{v+u}$ contiene una variación, entonces la sucesión $c_v, \ldots, c_{v+u}$ contiene a lo sumo una variación. Aún más, si $b_w, b_{w'}$ es la j-ésima variación de la sucesión de coeficientes de $g(x)$ y $c_t, c_{t'}$ es la j-ésima variación de la sucesión de coeficientes de $f(x)$, entonces $w \leqq u$ (Ejercicio 6) .Es así como la sucesión de b_j, tiene por lo menos tantas variaciones como la sucesión de c_j. Finalmente, dado que $b_0 = c_0$ y $g(0) = -rf(0)$, la sucesión de b_j [los coeficientes de $g(x)$] tiene más variaciones que la sucesión de c_j [los coeficientes de $f(x)$].

Si $f(x) = 0$ tiene raíces positivas $r_1, r_2, \ldots, r_k$, entonces

$$f(x) = (x - r_1)(x - r_2) \ldots (x - r_k)Q(x)$$

Por aplicaciones reiteradas del enunciado a que hemos hecho referencia, la sucesión de coeficientes de $f(x)$ tiene por lo menos k variaciones más que las de $Q(x)$, es decir, el número de variaciones de signo de $f(x)$ es $\geqq k$. De este modo una ecuación polinomia real con V variaciones en los signos de los coeficientes tiene, cuando más, V raíces positivas.

Ahora, si escribimos $f(x)$ en la forma

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_sx^{n-s},$$

en donde $0 \leqq s \leqq n$, podemos suponer que $a_0a_s \neq 0$. Luego,

$$f(x) = x^{n-s}(a_0x^s + a_1x^{s-1} + \cdots + a_s) = x^{n-s}g(x),$$

y las raíces positivas de $g(x) = 0$ son precisamente aquellas de $f(x) = 0$. Ya que $g(x)$ es continuo para todo x, la ecuación $g(x) = 0$ tiene un número par o impar, N, de raíces positivas (no necesariamente distintas) según que $0 < a_0a_s$, o que $a_0a_s < 0$ (Cap.

III - 13, Ejercicio 5). También V es par si $0 < a_0a_n$, e impar si $a_0a_n < 0$. Por consiguiente N y V son ambos pares o ambos impares, es decir,

TEOREMA IV-10. REGLA DE DESCARTES PARA LOS SIGNOS. *Un polinomio real con V variaciones en los signos de sus coeficientes, tiene $V - 2k$ raíces positivas (reales), siendo k un entero no negativo.*

Dado que las raíces negativas de $f(x) = 0$ son iguales a las raíces positivas de $f(-x) = 0$, excepto por el signo (Cap. IV - 8), también se tiene: *un polinomio real $f(x)$ tiene $W - 2k$ raíces negativas, siendo k un entero no negativo y W el número de variaciones de los signos de los coeficientes de $f(-x)$.*

Consideremos unos cuantos ejemplos de estos dos aspectos de la Regla de los Signos de Descartes. La ecuación polinomia $x^4 - x^2 + 1 = 0$ tiene o bien dos raíces positivas y una negativa o no positiva; o una raíz negativa y dos complejas. La ecuación polinomia $x^3 - x^2 + x - 1 = 0$ tiene o bien tres raíces positivas, o una positiva y dos complejas. Las raíces de la ecuación polinomia $x^5 + x^4 - 7x^3 + 5x^2 - x\sqrt{2} + 11 = 0$ caen dentro de uno de los tres casos siguientes: cuatro raíces positivas, una negativa, y ninguna compleja; dos raíces positivas, una negativa y dos complejas; ninguna raíz positiva, una negativa y cuatro complejas. En el caso del polinomio $x^3 - x^2 + x - 1 = (x - 1)(x^2 + 1)$, podemos encontrar los ceros 1, i, $-i$, y de este modo determinar cuál de los casos señalados se verifica. Para cualquiera ecuación polinomia con coeficientes reales, puede hacerse una determinación exacta del caso adecuado por medio del Teorema de Sturm (Cap. IV - 12) sin necesidad de encontrar las raíces.

También puede utilizarse la Regla de los Signos de Descartes con el objeto de establecer límites para las raíces reales de cualquiera ecuación polinomia con coeficientes reales, es decir, de *cualquiera ecuación polinomia real.* Supongamos $f(x) = (x - p)Q(x) + R$, $0 < p$ y que $Q(x)$ no tenga variaciones en los signos de sus coeficientes. Entonces, la ecuación $Q(x) = 0$ no tiene raíces positivas. Si también R tiene el mismo signo que los coeficientes de Q, entonces para $x = p$, $f(x) = R$, y para $x > p$, $Q(x)$ y $f(x)$ tienen el mismo signo que R, es decir, $f(x)$ no tiene ceros positivos

mayores que p. La prueba para un límite superior p se aplica más fácilmente por medio de la división sintética, donde los coeficientes de $Q(x)$ y R constituyen la tercera hilera. Entonces, la prueba es la siguiente: *si p es un número positivo tal que en la división sintética de $f(x)$ por $x - p$ todos los números de la tercera hilera tengan el mismo signo, o sean iguales a cero, entonces p es un límite superior para los ceros reales de $f(x)$.* Se puede determinar análogamente un límite inferior $-q$ para los ceros reales en donde q es un límite superior para los ceros de $f(-x)$.

Por ejemplo, si $f(x) = 2x^4 - 3x^3 - x^2 - 25x + 30$ y $p = 4$, tenemos

2	−3	−1	−25	30	4
0	8	20	76	204	
2	5	19	51	234	

de donde $f(x)$ no tiene ceros positivos mayores que 4. Análogamente, $f(x)$ no tiene ceros negativos menores que −1, ya que $f(-x) = 2x^4 + 3x^3 - x^2 + 25x + 30$ no tiene ceros positivos mayores que 1, de acuerdo con el cuadro siguiente:

2	3	−1	25	30	1
0	2	5	4	29	
2	5	4	29	59	

Hay todavía otros dos métodos conocidos (Bibliografía Nº 1; págs. 162-166) para determinar los límites superiores de las raíces reales de una ecuación polinomia real

$$p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = 0, \quad a_0 > 0.$$

Si $a_j \geqq 0$ $(j = 1, 2, \ldots, k-1)$, $a_k < 0$, y todos los coeficientes negativos son menores que o iguales a A en valor absoluto, luego $1 + \sqrt[k]{A/a_0}$, es un límite superior de las raíces reales de $p(x)$. Si el valor absoluto de cada a_j negativa se divide por la suma de todos los a_i positivos $(i < j)$ y B es el mayor cuociente obtenido de este modo, entonces $1 + B$ es un límite superior de los ceros reales de $p(x)$.

Informaciones generales más exactas sobre la ubicación de los ceros de cualquier polinomio real pueden hallarse en el Teorema de Sturm (Cap. IV - 12), que proporciona el número exacto de raíces distintas en cualquier intervalo $a < x \leqq b$.

EJERCICIOS

1. Discutir la naturaleza de las raíces de las ecuaciones siguientes:
   a) $x^5 + 3x^4 + 4x^3 + 2x - 6 = 0$;
   b) $x^4 - 15x^2 + 7x - 11 = 0$;
   c) $x^n - 1 = 0$ cuando n es impar, cuando n es par.
   d) $x^n + 1 = 0$ cuando n es impar, cuando n es par;

2. Determinar los límites superior e inferior de las raíces reales de las ecuaciones siguientes:
   a) $x^3 + 2x + 20 = 0$;
   b) $x^3 - 3x^2 - 2x + 5 = 0$;
   c) $3x^4 - 6x^3 + 8x - 3 = 0$

3. ¿Son los límites determinados en la respuesta al Ejercicio 2, los límites reales mejores posibles, los límites enteros mejores posibles?

4. Demostrar que el número de raíces negativas de $f(x) = 0$ es de la forma $P - 2k$, donde P es el número de permanencias de signo de $f(x)$, k es un entero no negativo, y $f(x)$ no tiene coeficientes cero.

5. Demostrar que si en la división sintética de $f(x)$ por $x - b$, $b < 0$, los signos de los términos de la tercera hilera, asociando el signo adecuado a términos cualesquiera que sean iguales a cero, pueden hacerse alternando mediante una elección adecuada de b, y si $f(x)$ es de grado par, entonces la ecuación $f(x) = 0$, no tiene raíces negativas menores que b.

6. Hacer por escrito una demostración completa del Teorema IV-10

IV-12 TEOREMA DE STURM. Consideraremos un método para determinar exactamente el número de ceros reales distintos de cualquier polinomio dado real en cualquier intervalo $a < x \leqq b$. En la sección siguiente este método se ampliará con el objeto de determinar el número de ceros de cualquiera multiplicidad dada k. Entonces, podremos determinar el número exacto (incluso multiplicidades) de raíces reales de cualquiera ecuación polinomia real dada $p(x) = 0$.

Dado cualquier polinomio real $f(x)$, podemos hacer $f_0 = f(x)$ y $f_1 = cf'(x)$, donde $f'(x)$ es la derivada de $f(x)$ (Cap. III - 14) y c es cualquiera constante positiva, frecuentemente el recíproco del máximo común divisor de los coeficientes de $f'(x)$. En seguida, aplicamos el Algoritmo de Euclides (Cap. III-7) a f_0 y f_1 con la modificación de que el signo de cada resto se cambie, es decir, hacemos

$$f_0 = q_1 f_1 - c_2 f_2,$$
$$f_1 = q_2 f_2 - c_3 f_3,$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$f_{k-2} = q_{k-1} f_{k-1} - c_k f_k,$$
$$f_{k-1} = q_k f_k.$$

Dado que los signos de las funciones tienen un significado, sólo pueden insertarse o eliminarse arbitrariamente los factores positivos. El esquema del Cap. III-7 puede modificarse para que resulte.

$$\begin{array}{cccccc} & q_1 & q_2 & q_3 & \cdots & q_k \\ f_0 & f_1 & f_2 & f_3 & \cdots & f_k \quad 0 \\ q_1 f_1 & q_2 f_2 & q_3 f_3 & q_4 f_4 & \cdots & \\ -c_2 f_2 & -c_3 f_3 & -c_4 f_4 & -c_5 f_5 & \cdots & \end{array}$$

donde los c son constantes positivas arbitrarias. Luego f_k es el máximo común divisor de f_0 y f_1 y un divisor común de f_j $(0 \leqq j \leqq k)$. El polinomio f_k no es necesariamente el máximo común divisor dado que es posible que su coeficiente inicial no sea $+1$.

Si $f_0 = x^5 - 24x^2 + 16x + 12$, podemos hacer $f_1 = x^3 - 12x + 4$, $f_2 = x^2 - x - 1$, $f_3 = 2x - 1$, $f_4 = 1$. En este caso, los polinomios f_0 y f_1 son primos entre sí. Si $f_0 = x^6 - 3x^2 - 2$, podemos hacer $f_1 = x^4 - x$, y $f_2 = x^2 + 1$. En este caso, f_3 es idénticamente nulo y f_2 es el máximo común divisor de f_0 y f_1. En general, la sucesión

$$f_0, f_1, f_2, \ldots, f_k,$$

donde f_k no es idénticamente nulo, se denomina la *sucesión cuociente* de f_0 y f_1. Formaremos también una sucesión de polinomios g_j, haciendo $g_j = f_j$ si f_k es constante; y $g_j f_k = f_j$ si f_k es de grado positivo. La sucesión

$$g_0, g_1, g_2, \ldots, g_k$$

se llama la *sucesión de Sturm* de f_0. Los g se denominan *funciones de Sturm* o *polinomios de Sturm* en f_0. Por ejemplo, la sucesión de Sturm del polinomio anterior $f_0 = x^4 - 24x^2 + 16x + 12$ puede formarse como sigue:

$$g_0 = x^4 - 24x^2 + 16x + 12,$$
$$g_1 = x^3 - 12x + 4,$$
$$g_2 = x^2 - x - 1,$$
$$g_3 = 2x - 1,$$
$$g_4 = 1$$

La sucesión de Sturm del polinomio $f_0 = x^5 - 3x^3 - 2$ citado anteriormente puede hacerse como sigue:

$$g_0 = x^4 - x^2 - 2,$$
$$g_1 = x^3 - x,$$
$$g_2 = 1.$$

La sucesión de Sturm de cualquier polinomio $f_0(x)$ con coeficientes reales tiene las siguientes propiedades:

(i) Si $f_0(x_1) = 0$, entonces $g_0g_1 < 0$ cuando $x = x_1$; y $g_0g_1 > 0$ cuando $x = x^+_1$, donde x^-_1 y x^+_1 indican, respectivamente, un valor de x ligeramente menor que x_1 y un valor apenas mayor que x_1. Es fácil imaginarse esta propiedad por medio del gráfico de $y = f^2_0$. Cuando f_0 es lineal, la ecuación $y = f^2_0$ tiene una sola raíz doble en $x = x_1$, el gráfico es una parábola, y $(d/dx)f^2_0 = 2cf^2_1 \cdot g_0g_1$ es negativa en x^-_1 y positiva en x^+_1, donde c es una constante positiva y f_1 es un polinomio real. En general, todo cero de f^2_0 tiene multiplicidad par (Cap. IV-13) y $(d/dx)f^2_0$ tiene las mismas propiedades que las que hemos considerado anteriormente en el caso especial.

(ii) Si algún $g_j(x_1) = 0$ donde $j > 0$, entonces $g_{j-1}g_{j+1} < 0$ en $x = x_1$. Esta desigualdad puede obtenerse de la identidad $f_{j-1} = q_jf_j - cf_{j+1}$, dado que todos los ceros comunes de f_{j-1} y f_j; o de f_j y de f_{j+1} deben ser ceros de f_k. Esta identidad tiene la forma $g_{j-1} = q_jg_j - cg_{j+1}$, donde $(g_{j-1}\ g_j) = 1 = (g_j,\ g_{j+1})$ cuando se expresa en función de los g, en que $f_j = f_kg_j$. Por consiguiente, $g_{j-1}g_{j+1} < 0$ todas las veces que $g_j = 0$.

(iii) El polinomio g_k es diferente de cero para todos los valores reales de x. Esta propiedad es una consecuencia inmediata de la definición de $g_k = 1$ cuando f_k no es constante y es igual a f_k cuando f_k es constante.

Si expresamos la primera propiedad de las citadas anteriormente por medio de la sucesión de signos de las funciones de Sturm, resulta que los primeros dos signos de la sucesión son $- +$ en x^-_1; y $+ +$ en x^+_1; o son $+ -$ en x^-_1; y $- -$ en x^+_1 donde x_1 es cualquier cero de f_0. La demostración hecha de la segunda propiedad señala que todas las veces que algún g_j $(j > 0)$ se anula, los polinomios g_{j-1} y g_{j+1} tienen signos opuestos, es decir, tenemos, $- 0 +$; o bien $+ 0$. La tercera propiedad indica que g_k no cambia nunca de signo. Intuitivamente, podemos imaginar las variaciones de los signos de la sucesión de Sturm de $f_0(x)$ que se des-

liza hacia la izquierda a medida que la variable real x crece. Por, ejemplo, consideremos los signos de la sucesión de Sturm citada anteriormente para $f_0 = x^4 - 24x^2 + 16x + 12$ para los valores indicados de x como se muestra en el cuadro siguiente:

x	g_0	g_1	g_2	g_3	g_4
−6	+	−	+	−	+
−4	−	−	+	−	+
−1	−	+	−	−	+
0	+	+	−	−	+
1	+	−	−	+	+
2	−	−	+	+	+
4	−	+	+	+	+
5	+	+	+	+	+

En realidad, la sucesión de Sturm de $f_0(x)$ será una sucesión de constantes para cualquier valor real de x, por ejemplo $x = a$. Usaremos el símbolo S_a para indicar el número de variaciones de la sucesión cuando $x = a$. De acuerdo con las propiedades (ii) y (iii) S_a no puede cambiar a medida que x pasa por cualquier cero de g_j $(j > 0)$ que no es un cero de g_0. De acuerdo con (i) si $f_0(x_1) = 0$, entonces (Cap. IV-13) $g_0(x_1) = 0$, y la sucesión tiene una variación de signo en sus primeros dos términos en $x = x^-_1$, pero ninguna variación en $x = x^+_1$. De este modo, S_a cambia solamente en los ceros de $f_0(x)$ y decrece en 1 todas las veces que x crece debido a los ceros de $f_0(x)$. Así, tenemos:

TEOREMA IV-11. TEOREMA DE STURM. *Un polinomio real $f(x)$ tiene exactamente $S_a - S_b$ ceros reales y distintos en el intervalo $a < x \leqq b$.*

Anteriormente, hemos dado la sucesión de Sturm del polinomio $x^4 - 24x^2 + 16x + 12$. Para valores negativos muy grandes de x, basta considerar los términos principales (Cap. IV-5) y las funciones de Sturm tienen los signos + − + − + con cuatro variaciones. Para valores positivos grandes de x, tenemos + + + + + sin ninguna variación. Por consiguiente, el polinomio $x^4 - 24x^2 + 16x + 12$ tiene cuatro ceros reales distintos.

La sucesión de Sturm g_0, g_1, g_2 de $f_0 = x^3 - 3x^2 - 2$ se obtuvo anteriormente dividiendo los polinomios f_0, f_1, f_2 por f_1, ya que f_2

no es una constante. Para valores negativos grandes de x sus signos son $+ \; - \; +$ con dos variaciones. Para valores positivos grandes de x sus signos son $+ \; + \; +$ sin ninguna variación. En consecuencia, el polinomio $x^4 - 3x^2 - 2$ tiene dos ceros reales y distintos.

El Teorema de Sturm también se puede emplear para determinar límites para las raíces de las ecuaciones polinomias y, por cierto, sirve también para aislar las raíces en pequeños intervalos arbitrarios. Por ejemplo, $x^4 - 3x^2 - 2 = 0$ tiene dos raíces reales distintas, según se determinó anteriormente. En $x = 2$ los signos de las funciones de Sturm correspondientes, son $+ \; + \; +$, lo mismo que para valores positivos grandes de x. Por consiguiente, según el Teorema IV-11, la ecuación $x^4 - 3x^2 - 2 = 0$ no tiene raíces reales mayores que 2. Análogamente, en $x = -2$ los signos son $+ \; - \; +$, los mismos que para valores negativos muy grandes de x, y no hay raíces reales menores que -2. En $x = 1$, 0, y -1 los signos de las funciones de Sturm que son diferentes de cero, es decir, los signos de las funciones de Sturm que tienen signos, son $- \; +$ con una variación. Por consiguiente, $S_{-2} = 2$; $S_{-1} = 1$; $S_0 = 1$; $S_1 = 1$, y $S_2 = 0$, de donde resulta un raíz real que satisface $-2 < x < -1$ y una raíz real que satisface $1 < x < 2$. Los intervalos $-2 < x \leqq -1$ y $1 < x \leqq 2$ se reemplazaron por $-2 < x < -1$ y $1 < x < 2$, ya que $x = -1$ y $x = 2$ no son raíces. El procedimiento de encontrar intervalos que contengan las raíces podría continuar, por medio de S_1^1, S_1^2, ... En general, diremos que las raíces reales de una ecuación se *han aislado* cuando se ha encontrado un intervalo $a < x < b$ para cada raíz real tal que $b - a \leqq 1$ y cuando el intervalo contiene sólo una de las raíces distintas.

Ahora podemos determinar exactamente el número de raíces reales distintas de cualquiera ecuación polinomia real, es decir, de cualquiera ecuación polinomia $p(x) = 0$ con coeficientes reales. También podemos aislar cada raíz en un intervalo tan pequeño como se desee. En la sección siguiente definiremos la multiplicidad de una raíz y determinaremos el número total de raíces reales en cualquier intervalo, por medio de su multiplicidad.

EJERCICIOS

1. Encontrar las raíces reales de:
   a) $x^4 - 6x^3 + 7x^2 + 6x - 2 = 0$ (Ver Ejercicio 4, Cap. III-7);
   b) $x^4 - 2x^2 + 12x - 8 = 0$;

c) $x^4 - 13x^2 + 4x + 2 = 0$;

d) $x^4 - x^3 + 10x - 4 = 0$.

2. Aislar, por medio del Teorema de Sturm, todas las raíces reales:

a) $x^3 + 2x + 20 = 0$;

b) $x^4 - 3x^3 - 2x + 5 = 0$;

c) $3x^4 - 6x^3 + 8x - 3 = 0$.

IV-13 RAICES MULTIPLES. Hemos definido (Cap. IV-1) un número b como un cero de un polinomio $p(x)$ si y sólo si $p(b) = 0$. En consecuencia, 2 es un cero de $x - 2$, de $x^2 - 4x + 4$, de $x^3 - 3x + 2$, y de $x^3 - 2x^2 + 4x - 8$. Esta definición junto con el Teorema IV-1 implican que cualquier polinomio $p(x)$ con un cero b puede escribirse en la forma $p(x) = (x - b) \cdot q(x)$, donde $q(x)$ es un polinomio. En los ejemplos anteriores, $x - 2 = (x - 2) \cdot 1$; $x^2 - 4x + 4 = (x - 2) \cdot (x - 2)$; $x^2 - 3x + 2 = (x - 2) \cdot (x - 1)$; y $x^3 - 2x^2 + 4x - 8 = (x - 2) \cdot (x^2 + 4)$. En otras palabras, b es una raíz de $p(x) = 0$, si y sólo si $x - b$ es divisor de $p(x)$. Se dice que b es una *raíz múltiple* de $p(x) = 0$ si y sólo si $(x - b)^2$ es divisor de $p(x)$. Por eso, 0 es una raíz múltiple de $x^4 - 7x^3$.

También nos referiremos a la multiplicidad de una raíz b de $p(x) = 0$ para indicar la mayor potencia entera de $(x - b)$ que es divisor de $p(x)$. Así, por ejemplo, la raíz 0 tiene multiplicidad 5 en $x^8 - 7x^7 + x^6 = 0$. En general, una raíz b de $p(x) = 0$ tiene *multiplicidad* k si $(x - b)^k$ es divisor de $p(x)$ y $(x - b)^{k+1}$ no es divisor de $p(x)$, donde k es un entero positivo. Una raíz de multiplicidad 1 se denomina *raíz simple*.

El cálculo de la multiplicidad de una raíz b suele efectuarse más fácilmente por medio de un cambio de variable para expresar $p(x)$ en la forma $q(x - b)$. Esto puede hacerse mediante la división sintética (Cap. IV-3) o mediante la fórmula de Taylor (Cap. III-14). En la notación de la fórmula de Taylor, tenemos la siguiente identidad para cualquier polinomio $f(x)$:

$$f(x) = f(a) + f'(a)(x - a) + \cdots + f^{(n)}(a)\frac{(x - a)^n}{n!}.$$

Es evidente ahora que si $f(a) = 0$, entonces $f(x)$ tiene $(x - a)$ como factor; si $f(a) = f'(a) = 0$, entonces $(x - a)^2$ es un factor de $f(x)$; y en general, si $f(a) = f'(a) = \cdots = f^{(k)}(a) = 0$, entonces $(x - a)^{k+1}$ es un factor de $f(x)$. Dado que los coeficientes de la fórmula de Tay-

lor están determinados unívocamente, la proposición conversa es también verdadera, es decir, si $(x - a)^{k+1}$ es un factor de $f(x)$, entonces $f(a) = f'(a) = \ldots = f^{(k)}(a) = 0$. Además, si $(x - a)^{k-1}$ es factor de $f(x)$, entonces $f'(x)$ tiene a $(x - a)^k$ como factor y $(x - a)^{k-1}$ es factor de $f''(x)$ y así sucesivamente. Por consiguiente, cualquiera raíz de $f(x) = 0$ de multiplicidad $m > 1$ es una raíz de $f'(x) = 0$ de multiplicidad $m-1$. En particular, una raíz simple de $f(x) = 0$, no es una raíz de $f'(x) = 0$. Si $f(x) = 0$ y $f'(x) = 0$ tienen una raíz común r que es un cero de $f'(x)$ de multiplicidad $m - 1$, entonces r es un cero de $f(x)$ de multiplicidad m. Finalmente, si $f_k(x)$ es el máximo común divisor de $f(x)$ y $f'(x)$ y $f = f_k g_k$, entonces $g_k(x)$ tiene los mismos ceros distintos que $f(x)$, pero no raíces múltiples. En consecuencia en el Cap. IV - 12 los ceros de $g_0(x)$ son simples y son precisamente las raíces distintas de $f_0(x)$. También, $f_0(x)$ tiene raíces múltiples si y sólo si $f_k(x)$ es de grado positivo.

Dado cualquier intervalo $a < x \leqq b$ y cualquier polinomio real $f_0(x)$, podemos encontrar la sucesión cuociente de $f_0(x)$, es decir, $f_0, f_1, \ldots, f_{k1}$. Ya que f_{k1} es un asociado del máximo común divisor de f_0 y f'_0, f_{k1} es una constante si y sólo si $f_0(x)$ tiene solamente raíces simples. Si f_{k1} tiene grado positivo, la sucesión de Sturm $g_0, g_1, \ldots, g_{k1}$ se denomina la primera sucesión Sturm de f_0. En ambos casos, el Teorema IV - 11 proporciona el número de las raíces reales distintas, es decir, el número N_1 de ceros de $f_0(x)$ de multiplicidad por lo menos uno. Ahora, tendremos en cuenta que cualquier cero de $f_0(x)$ de multiplicidad m es un cero de $f'_0(x)$ y por lo tanto de $f_{k1}(x)$ de multiplicidad $m - 1$. Por consiguiente, si f_{k1} no es una constante, encontraremos su sucesión cuociente $f_{k1}, f'_{k1}, \ldots, f_{k2}$ y su sucesión Sturm, la segunda sucesión Sturm de f_0. Si $f_{k2} = c(f_{k1}, f'_{k1})$ es constante, $f_0(x)$ no tiene raíz de multiplicidad mayor que dos. En todo caso, el Teorema IV - 11 para f_{k1} proporciona el número N_2 de ceros de $f_0(x)$ de multiplicidad por lo menos dos. Si f_{k2} tiene grado positivo, podemos encontrar su sucesión Sturm (la tercera sucesión Sturm de f_0) y el número N_3 de ceros de multiplicidad por lo menos tres. Dado que $f_0(x)$ tiene grado finito, este procedimiento puede repetirse sólo un número finito de veces. Si N_i es el número de ceros de $f_0(x)$ de multiplicidad por lo menos i, que se ha obtenido de la i-ésima sucesión de Sturm de f_0, entonces el número de ceros de multiplicidad exactamente j es $N_j - N_{j+1}$. En particular, el número de raíces simples es $N_1 - N_2$. De este procedimiento

resulta el *Teorema de Sturm para las raíces múltiples* (Bibliografía Nº 48) por medio del cual el número $N_j - N_{j+1}$ de raíces reales de $f_0(x)$ en cualquier intervalo $a < x \leqq b$ y de cualquiera multiplicidad j puede calcularse sin necesidad de determinarse las raíces mismas.

Los ceros de $h_1 = f_0/f_{k1}$ son los ceros (reales o imaginarios) de f_0 de multiplicidad por lo menos uno; los ceros de $h_2 = f_{k1}/f_{k2}$ son los ceros de f_0 de multiplicidad por lo menos dos; los de $h_j = f_{k(j-1)}/f_{kj}$ son los ceros de f_0 de multiplicidad por lo menos j. Por lo tanto, los ceros de $s_1 = h_1/h_2$ son precisamente los ceros simples de f_0; los ceros de $s_2 = h_2/h_3$ son las raíces dobles; los de $s_j = h_j/h_{j+1}$ son los ceros de multiplicidad j, en que $s_n = h_n$ si f_{kn} es constante. Los f_{kj} son polinomios que se obtienen por el procedimiento del máximo común divisor; los h_j y los s_j son polinomios que se obtienen por división. Estas operaciones pueden efectuarse si $f_0(x)$ tiene coeficientes reales o complejos. Por consiguiente para cualquiera ecuación polinomia $f(x) = 0$ y para cualquier entero positivo j podemos obtener una ecuación polinomia $s_j = 0$ cuyas raíces son las raíces distintas (reales o imaginarias) de $f(x)$ de multiplicidad j. Luego, mediante estos polinomios s_j se tiene

TEOREMA IV - 12. *Una ecuación polinomia $f(x) = 0$ puede resolverse: (i) por medio de la fórmula cuadrática si tiene a lo sumo dos raíces de cada multiplicidad k; y (ii) por medio de sus coeficientes y extracción de raíces si tiene a lo más cuatro raíces de cada multiplicidad k.*

EJEMPLO. La ecuación

$$f_0(x) = x^{10} - x^8 - 5x^6 + x^4 + 8x^2 + 4 = 0 \qquad \text{(IV - 10)}$$

tiene a lo sumo dos raíces positivas y máximo dos raíces negativas (Cap. IV - 11). No tiene raíces racionales (Teorema IV - 9). Antes de sacar el máximo común divisor para obtener las sucesiones de Sturm, calculamos las sucesiones cuocientes:

$$\begin{aligned} f_0 &= x^{10} - x^8 - 5x^6 + x^4 + 8x^2 + 4, \\ f_1 &= 5x^9 - 4x^7 - 15x^5 + 2x^3 + 8x, \\ f_2 &= x^8 + 10x^6 - 3x^4 - 32x^2 - 20, \\ f_3 &= x^7 - 3x^3 - 2x, \\ f_{41} &= -x^6 + 3x^2 + 2; \end{aligned}$$

$$
\begin{aligned}
f_{k1} &= -x^6 + 3x^2 + 2,\\
c_1 f'_{k1} &= -x^5 + x,\\
f_{k2} &= -x^2 - 1;
\end{aligned}
$$

$$
\begin{aligned}
f_{k2} &= -x^2 - 1,\\
c_2 f'_{k2} &= -x,\\
f_{k3} &= 1;
\end{aligned}
$$

donde f_{k1} es el máximo común divisor (MCD) de f_0 y f'_0, f_{k2} es un MCD de f_{k1} y de f'_{k1}; y f_{k3} es un MCD de f_{k2} y de f'_{k2} (es decir, f_{k2} y f'_{k2} son primos entre sí).

Luego la primera sucesión de Sturm de (IV - 10) es:

$$
\begin{aligned}
g_{10} &= -x^4 + x^2 + 2 = f_0/f_{k1},\\
g_{11} &= -5x^3 + 4x = f_1/f_{k1},\\
g_{12} &= -x^2 - 10 = f_2/f_{k1},\\
g_{13} &= -x = f_3/f_{k1},\\
g_{14} &= 1 = f_{k1}/f_{k1};
\end{aligned}
$$

la segunda sucesión de Sturm es

$$
\begin{aligned}
g_{20} &= x^4 - x^2 - 2 = f_{k1}/f_{k2},\\
g_{21} &= x^3 - x = c_1 f'_{k1}/f_{k2},\\
g_{22} &= 1 = f_{k2}/f_{k2};
\end{aligned}
$$

y la tercera sucesión de Sturm es

$$
\begin{aligned}
g_{30} &= -x^2 - 1 = f_{k2},\\
g_{31} &= -x = c_2 f'_{k2},\\
g_{32} &= 1 = f_{k3}.
\end{aligned}
$$

Según la primera sucesión de Sturm vemos que (IV - 10) tiene dos raíces reales distintas, una positiva y una negativa, dado que $S_{-\infty} = 3$, $S_0 = 2$, y $S_\infty = 1$. Análogamente, según la segunda sucesión de Sturm vemos que (IV - 10) tiene dos raíces reales distintas de multiplicidad por lo menos dos, una positiva y una negativa. Según la tercera sucesión de Sturm, se ve que no hay raíces reales de multiplicidad mayor que dos.

En la notación del párrafo anterior al Teorema IV - 12, los ceros de

$$h_1 = -x^4 + x^2 + 2 = f_0/f_{k1}$$

son los ceros de f_0 de multiplicidad por lo menos uno; los ceros de

$$h_2 = x^4 - x^2 - 2 = f_{k1}/f_{k2}$$

son los ceros de f_0 de multiplicidad por lo menos dos; y los ceros de

$$h_3 = -x^2 - 1 = f_{k2}/f_{k3}$$

son los ceros de f_0 de multiplicidad por lo menos tres. Nótese que $h_j = g_{jo}$, dado que ambos están determinados de la misma manera. Continuando con la notación anterior, los ceros de

$$s_1 = -1 = h_1/h_2$$

son los ceros de f_0 de multiplicidad exactamente uno; los ceros de

$$s_2 = -x^2 + 2 = h_2/h_3$$

son los ceros de f_0 de multiplicidad exactamente dos; y los ceros de

$$s_3 = -x^2 - 1 = h_3$$

son los ceros de f_0 de multiplicidad exactamente tres. Según s_1, la ecuación (IV - 10) no tiene raíces simples; según s_2 tiene como raíces dobles $\sqrt{2}$ y $-\sqrt{2}$; según s_3 tiene como raíces triples i, $-i$. Por consiguiente las raíces de (IV - 10) son $\sqrt{2}$, $\sqrt{2}$, $-\sqrt{2}$, $-\sqrt{2}$, i, i, i, $-i$, $-i$, $-i$.

El cálculo de las series de Sturm de un polinomio suele ser un procedimiento largo y tedioso. Sin embargo, la resolución de una ecuación cúbica o de cuarto grado por medio de fórmulas es también un proceso largo (Cap. IV - 9 y Cap. IV - 10). El Teorema IV - 11 y los métodos anteriores pueden aplicarse a cualquier polinomio con coeficientes complejos, cualquiera que sea su grado, con el objeto de obtener raíces múltiples y también simples todas las veces que sea posible resolver s_3 mediante nuestros métodos anteriores. Los s_j tienen grados menores que el polinomio dado si y sólo si hay raíces múltiples. En particular, si todas las raíces son raíces simples, entonces s_1 es un polinomio asociado del polinomio dado. Los métodos que se han presentado en esta sección son importantes porque nos permiten la resolución de ecuaciones que no

podrían ser hechas por los métodos estudiados anteriormente. En la sección siguiente y final de este capítulo consideraremos métodos de aproximación de raíces reales de ecuaciones polinomias en una variable con coeficientes reales.

EJERCICIOS

1. Resolver:

(a) $x^4 - 4x^3 - 2x^2 + 12x + 9 = 0$,
(b) $x^4 - 2x^3 - 3x^2 + 4x + 4 = 0$,
(c) $x^4 - 9x^3 + 9x^2 + 81x - 162 = 0$,
(d) $x^4 - 6x^2 - 8x - 3 = 0$,
(e) $x^3 - 7x^2 + 15x - 9 = 0$.

2. Resolver:

$x^{10} - 5x^9 - 5x^8 + 45x^4 - 108 = 0$

3. Proponer un método para resolver la ecuación del Ejercicio 2, encontrando primero las raíces racionales de una ecuación relacionada con ella.

IV-14 SOLUCIONES APROXIMADAS. Concluiremos nuestro breve estudio de la teoría de las ecuaciones con una discusión de dos métodos para calcular aproximadamente las raíces reales de una ecuación polinomia $f(x) = 0$ con coeficientes reales. Mediante el Teorema de Sturm o aún por el método de ensayo y error podemos determinar intervalos de la forma $n < x \leqq n + 1$ en el cual se encuentran las raíces (Cap. IV-12). Los procedimientos siguientes consisten en dos métodos para obtener aproximaciones sucesivas que tienden a la raíz como un límite. Dado que mediante el Teorema IV-9, puede obtenerse todas las raíces racionales, los métodos por aproximación serán necesarios solamente para las raíces irracionales.

Método de Newton. Supongamos que $f(x) = 0$ tiene una raíz $a + h$ en que el número a es conocido, $f'(a) \neq 0$, y h^2 es menor que uno. La fórmula de Taylor en $x = a + h$ da

$$f(a + h) = f(a) + f'(a)h + \frac{f''(a)}{1 \cdot 2} h^2 + \cdots = 0,$$

ya que $a + h$ es una raíz. Para valores pequeños de h, los términos que contienen h^2 como factor, se pueden despreciar y resulta $f(a) + f'(a)h = 0$, o $h = -f(a)/f'(a)$ como una primera aproximación para h, y $a_1 = a - f(a)/f'(a)$ como una primera aproximación para la raíz $a + h$. Este proceso se repite haciendo $a_2 = a_1 - f(a_1)/f'(a_1)$ y, en general, $a_{j+1} = a_j - f(a_j)/f'(a_j)$. Aunque a_j debe elegirse tal que $f'(a_j) \neq 0$, esto no causa ninguna dificultad, ya que $f'(x)$ tiene sólo un número finito de ceros. Por consiguiente si $f'(x) = 0$ para algún valor de $x = a_j$, simplemente se reemplaza a_j por un valor ligeramente diferente en el cual $f'(x) \neq 0$. La sucesión de valores $a, a_1, a_2, \ldots a_j \ldots$ tiende a $a + h$ como límite, al que se puede aproximar con el grado de precisión que se desee. Por ejemplo: $f(x) = x^5 - 3x + 1 = 0$ tiene una raíz entre cero y uno; $f'(x) = 5x^4 - 3$. Si $a = 0$, las diferencias $a_1 - a = \frac{1}{3}$; $a_2 - a_1 = .0014$, tienden a cero muy rápidamente y la raíz deseada es aproximadamente 0. 3346. El método de Newton puede también usarse para cualquiera función $f(x)$ que tenga una primera derivada.

El segundo método por aproximación, *el método de Horner*, proporciona los dígitos sucesivos en el desarrollo decimal de la raíz. Por ejemplo, $x^3 - 12x^2 + 5x - 17 = 0$ puede determinarse mediante el Teorema de Sturm o por ensayo y error con el objeto de obtener una raíz entre 10 y 20. En consecuencia, el primer dígito de la raíz se considera 1. Empleamos en seguida la división sintética, como en el Cap. IV - 3, con el objeto de disminuir las raíces en 10:

1	−12	5	−17	| 10
0	10	−20	−150	
1	−2	−15	−167	
0	10	80		
1	8	65		
0	10			
1	18			
0				
1				

y buscamos una raíz de la nueva ecuación $y^3 + 18y^2 + 65y - 167 = 0$, que tenga un valor entre 0 y 10, y encontramos que esta raíz está entre 1 y 2. Por eso el segundo dígito de la raíz es 1. En con-

secuencia, disminuimos las raíces en 1 y buscamos una raíz de la nueva ecuación $z^4 + 21z^3 + 104z - 83 = 0$, entre 0 y 1, y encontramos que está entre .6 y .7; disminuimos las raíces en .6 y buscamos una raíz de la nueva ecuación que se encuentre entre cero y un décimo. Continuando este procedimiento, se puede calcular un número finito de lugares decimales de la raíz buscada, 11.6... Después de las primeras etapas, puede obtenerse una aproximación útil del dígito siguiente considerando solamente los últimos dos términos de la ecuación de que se trate. Las raíces negativas de $f(x) = 0$ pueden calcularse cambiando los signos de las raíces positivas de $f(-x) = 0$.

Existen otros métodos de aproximación de raíces (Bibliografía Nº 49; págs. 151-180), como también reglas para reducir el trabajo en los procedimientos anteriores. Sin embargo, se ha presentado lo suficiente para indicar cómo se puede determinar cualquiera raíz real de una ecuación polinomia real con una aproximación de tantos lugares decimales como se desee. Para mayores detalles sobre éste y otros temas mencionados en este capítulo el lector puede consultar un texto sobre teoría de las ecuaciones.

En el presente capítulo hemos examinado algunos métodos para encontrar los ceros de un polinomio en una variable; hemos presentado fórmulas para determinar las raíces de ecuaciones polinomias de grados 1, 2, 3, y 4 (Cap. IV, Secciones 5, 9, y 10) con coeficientes complejos; considerado las ecuaciones polinomias de grado arbitrario teniendo en cuenta sus raíces múltiples y las ecuaciones polinomias reales de grado arbitrario respecto de sus raíces racionales. El estudio de los polinomios y las ecuaciones polinomias es la meta que nos habíamos propuesto alcanzar al ocuparnos de nuestro sistema de números, de la teoría de los números y de la teoría de los polinomios, y aunque representa un avance notable en nuestro propósito, no es de manera alguna la etapa final. A medida que progresamos en nuestro estudio se nos presentaron oportunidades de dedicar especial atención y desarrollar interesantes conceptos. Hemos considerado solamente algunos conceptos fundamentales básicos dentro del vasto campo del álgebra. El camino está ahora expedito para abordar una gran variedad de materias de las cuales podremos seleccionar sólo algunas.

Los tres capítulos restantes pueden leerse en cualquier orden según el interés del lector. El más importante es el Capítulo V

sobre matrices y determinantes y sus aplicaciones a la dependencia lineal, a la resolución de sistemas de ecuaciones lineales y a las transformaciones geométricas. El Capítulo VI contiene una aplicación importante de nuestras teorías algebraicas a los problemas clásicos de construcción en geometría y, en particular, una demostración de la imposibilidad de trisectar un ángulo arbitrario dado utilizando únicamente la regla y el compás. Por último, el Capítulo VII es una introducción a la representación gráfica de funciones, que corresponde, en cierto modo, al estudio de los conjuntos de funciones que figura en el Capítulo III.

EJERCICIOS

1. Calcular las raíces de $x^3 - 3x^2 - 2x + 5 = 0$, con una aproximación de cuatro cifras decimales.

2. Calcular la raíz real de $x^3 + 2x + 20 = 0$, con una aproximación de cinco cifras decimales.

3. El asta de una bandera mide cien pies de altura y se halla a diez pies de distancia de un poste de diez pies de altura. Si el asta se quiebra —sin que la sección superior se separe de la base— y de modo que toque el extremo superior del poste y roce la tierra, calcular la altura en que se quebró.

CAPITULO V

Determinantes y matrices

Los determinantes y las matrices tienen muchas aplicaciones prácticas en matemáticas y en otras ciencias. Examinaremos primero su desarrollo histórico (Cap. v-1), en seguida definiremos los determinantes mediante matrices (Cap. v-2) y permutaciones (Cap. v-3 a Cap. v-6), estudiaremos algunas de sus propiedades (Cap. v-7 a Cap. v-10), y consideraremos varias de sus aplicaciones. En particular, consideraremos el uso de los determinantes y de las matrices en la resolución de sistemas de ecuaciones lineales (Cap. v-11 y Cap. v-12); en la dependencia lineal (Cap. v-13); en la geometría analítica (Cap. v-14); y en las transformaciones geométricas (Cap. v-15).

V-1 DESARROLLO HISTORICO. La primera noción de un determinante se debió probablemente a Leibniz a fines del siglo diecisiete. El empleó símbolos análogos a nuestra actual notación de determinantes para simplificar las expresiones que se originan en la resolución de sistemas de ecuaciones lineales. Por ejemplo, consideremos el sistema siguiente de ecuaciones lineales de dos variables:

$$a_1x + b_1y = c_1,$$
$$a_2x + b_2y = c_2.$$

Si se multiplica la primera ecuación por $+b_2$, la segunda por $-b_1$, y si se suman las ecuaciones resultantes, obtenemos $(a_1b_2 - a_2b_1)x = c_1b_2 - c_2b_1$, o en la notación de los determinantes

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} x = \begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix},$$

que puede resolverse respecto de x si $a_1b_2 - a_2b_1 \neq 0$. Este procedimiento fue expresado como una regla formal para sistemas de n ecuaciones lineales de n variables por Gabriel Cramer en 1750. Por consiguiente, este método se denomina la Regla de Cramer (Cap. v - 11). Esta regla expresa una de las primeras aplicaciones básicas de los determinantes.

Durante dos siglos, desde la formulación de la Regla de Cramer, los determinantes se usaron de muchas maneras. Algunas de estas aplicaciones se examinarán en el presente capítulo; muchas otras no pueden apreciarse hasta que el lector no haya estudiado la rama particular de las matemáticas en la cual se emplea. Bézout (1799) usó determinantes en su método de eliminación por medio de ecuaciones lineales. Sylvester (1840) empleó determinantes en su método dialítico de eliminación. Se ha reconocido el trabajo de Vandermonde, Jacobi y otros en la teoría de los determinantes, asociando sus nombres con tipos especiales de determinantes. Por ejemplo, el determinante de Vandermonde (Ejercicio 22, Cap. v - 9) puede usarse en la discusión de las raíces de una ecuación cúbica. Los determinantes wronskianos y jacobianos tienen importancia en las teorías de matemáticas superiores. Los determinantes resultantes, eliminantes, alternantes, ortogonales, simétricos, orlados, son algunos de los muchos otros tipos de determinantes que tienen aplicaciones especiales en las teorías matemáticas.

Cauchy (1815) y Jacobi (1841) aportaron valiosas contribuciones a la teoría general de los determinantes. Poco tiempo después, el concepto de una ordenación cuadrada denominada determinante se amplió y surgió el concepto completamente diferente de una ordenación rectangular denominada matriz. La matriz es hoy el concepto fundamental con numerosas aplicaciones teóricas y prácticas. Toda matriz cuadrada con elementos pertenecientes a un anillo tiene asociado un determinante. La teoría de los determinantes ha llegado a ser una parte de la teoría de las matrices. Restringiremos nuestro estudio de las matrices a los conceptos necesarios en las aplicaciones a que nos hemos referido al comienzo de este capítulo. Otras aplicaciones y mayores detalles sobre la teoría pueden consultarse en textos tales como los N.os 9, 16, 39, 44 y 49 de la Bibliografía.

V-2 MATRICES. Una *matriz* se define como una ordenación rectangular tal como

$$\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \end{bmatrix},$$

y, en general,

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix}, \tag{V—1}$$

donde los elementos a_{ij} pueden pertenecer a cualquier conjunto dado de números, de polinomios o pueden ser elementos de un anillo dado de elementos. Nos preocuparemos principalmente de matrices cuyos elementos sean números reales o polinomios. También podrían considerarse matrices cuyos elementos pertenezcan a un anillo o a un campo arbitrario con sólo pequeñas modificaciones en nuestro presente estudio.

La matriz (v - 1) tiene m filas y n columnas. Se ha elegido la notación a_{ij} de modo que el primer subíndice *(índice de la fila)* designa la fila y el segundo subíndice *(índice de la columna)* designa la columna en la cual se encuentra el elemento. Por ejemplo, a_{12} se encuentra en la primera fila y en la segunda columna; a_{31} se encuentra en la tercera fila y en la primera columna; a_{ij} está en la i-ésima fila y en la j-ésima columna.

Cuando $m = n$, tenemos una *matriz cuadrada* tal como

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \qquad \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix},$$

o, en general,

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}. \tag{V—2}$$

En el Cap. v - 7 usaremos las permutaciones de los subíndices de los elementos y asociaremos un polinomio de los elementos de una

cualquiera matriz cuadrada con un polinomio de los elementos de esa matriz. Este polinomio se denominará el *determinante* de la matriz. Si los elementos de una matriz cuadrada son números, el determinante de la matriz es también un número.

El determinante de una matriz está definido sólo para matrices cuadradas y puede designarse empleando líneas rectas en lugar de los paréntesis cuadrados con que se designa una matriz. Por ejemplo, el determinante de la matriz

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

puede designarse por

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}. \tag{V–3}$$

La matriz (v - 1) puede también designarse por $[a_{ij}]$, $i = 1, 2, \ldots, m$; $j = 1, 2, \ldots, n$. La matriz cuadrada (v - 2) puede designarse por $[a_{ij}]$, $i, j = 1, 2, \ldots, n$ o simplemente como $[a_{11}, a_{22}, \ldots, a_{nn}]$ tomando en cuenta sus elementos con índices de fila y columna iguales, es decir, los elementos de su *diagonal principal*. El determinante de (v - 2) puede designarse empleando líneas rectas como en (v - 3); o también por $|a_{ij}|$, $i, j = 1, 2, \ldots, n$; o también por $|a_{11}, a_{22}, \ldots, a_{nn}|$. Presentamos estas tres notaciones para matrices y determinantes con el objeto de facilitar la consulta de otros textos sobre matrices y determinantes. Desgraciadamente, la notación matemática no se ha uniformado bien. Con todo, el conocimiento de las diferentes notaciones que hemos señalado permitirá al lector reconocerlas rápidamente en cualquier otro texto. Nosotros emplearemos, en las tres notaciones, líneas rectas para los determinantes y paréntesis cuadrados para las matrices.

Hasta aquí hemos definido una matriz y hemos señalado que, por medio de permutaciones, puede asociarse un determinante a toda matriz cuadrada. En algunas de las secciones que siguen definiremos y estudiaremos algunas propiedades de las permutaciones.

EJERCICIOS

1. Escribir cinco matrices.

2. ¿Se pueden asociar determinantes con alguna de las matrices dadas en el Ejercicio 1? Indicar estos determinantes en los casos en que sea posible.

3. Dar ejemplos de cuatro matrices cuadradas y designar el determinante asociado con cada una de ellas.

4. El orden de una matriz cuadrada (Cap. v-7) es igual al número de elementos de su diagonal principal. Indicar el orden de cada una de las matrices dadas en el Ejercicio 3.

5. Dar ejemplos de tres matrices cuadradas de diferente orden.

6. Designar de tres maneras el determinante de la matriz $[a_{11}, a_{22}, a_{33}, a_{44}]$.

7. Dar un ejemplo de una matriz de tercer orden, cuyos elementos sean números complejos.

8. Dar un ejemplo de una matriz de tercer orden, cuyos elementos sean polinomios en x de grado positivo.

9. Proponer matrices que tengan una de las siguientes propiedades: (a) dos filas y tres columnas; (b) una fila y tres columnas; (c) tres filas y una columna; (d) una fila y una columna.

V-3 PERMUTACIONES. Se llaman *permutaciones* de un conjunto dado cualquiera, las diferentes disposiciones en que se pueden ordenar, en una fila, los elementos del conjunto. Por ejemplo, dados los enteros 1 y 2, tenemos dos permutaciones 1, 2 y 2, 1; dados los enteros 1, 2, 3, tenemos seis permutaciones 123, 132, 213, 231, 321 y 312 en las que se han suprimido las comas por comodidad. Omitiremos estas comas cada vez que sea posible sin producir confusión al lector. Sin embargo, dados dos enteros tales como 11 y 17, no podremos, por supuesto, omitir las comas al escribir las dos permutaciones 11, 17 y 17, 11.

Consideremos el número P_n de permutaciones de un conjunto dado de n elementos distintos. $P_2 = 2$, ya que dos elementos cualesquiera a y b pueden disponerse de dos maneras: ab y ba. Puede introducirse un tercer elemento c en cada una de estas dos permutaciones, de tres maneras: antes de cada elemento o después de ambos, resultando así $3 \cdot 2 = 6$ permutaciones de los tres elementos. Se escribe $P_3 = 3!$ De modo análogo, dado cualquier entero positivo k, se puede introducir un elemento adicional en cada una de las permutaciones de k elementos en $k + 1$ maneras diferentes: antes de cada elemento y después de todos ellos. De esta manera, si P_k denota el número de permutaciones de k elementos, entonces $P_{k+1} = (k + 1)P_k$. Por eso $P_4 = 4!$, $P_5 = 5!$, ..., $P_n = n!$ para todos los valores enteros positivos de n (Ejercicio 1).

Hasta aquí hemos definido una permutación como una ordenación lineal, tal como

1 2 3 4 5 6 7 8 9 10 11 12

en contraste con una ordenación circular (como por ejemplo en un reloj, Fig. v - 1) u otra ordenación de cualquier conjunto dado de elementos,

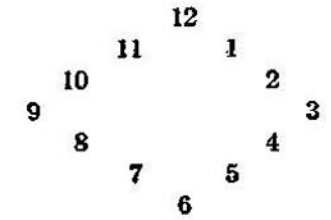


FIG. V—1

Consideraremos, en seguida, un orden (permutación) del conjunto dado de elementos como su *orden natural* y todas las permutaciones de estos elementos se considerarán con respecto a su orden natural. Por ejemplo, es costumbre admitir que el orden natural de cualquier conjunto de números enteros positivos consecutivos, es el orden que se usa al contar; que el orden natural de cualquier conjunto finito de números reales es el orden creciente de sus valores numéricos; que el orden natural de cualquier conjunto de letras de un alfabeto es su orden alfabético. Por eso consideraremos que cada una de las permutaciones

(V - 4) 12345, 3567, acflm

se encuentran en su orden natural. Por la misma razón, cada una de las permutaciones

(V - 5) 21345, 3576, afchm

se encuentra en una disposición diferente de su orden natural. Esta diferencia, o sea la relación entre dos permutaciones tales como 12345 y 21345 de un conjunto dado de elementos, puede expresarse por medio de inversiones (Cap. v - 4).

EJERCICIOS

1. Hacer una demostración completa por inducción matemática (Cap. 1-4) de que $P_n = n!$ para cualquier entero positivo n.
2. Hacer una lista de todas las permutaciones del conjunto de letras *cat*.
3. Hacer una lista de las 24 permutaciones del conjunto de letras *duck*.

V - 4 INVERSIONES. Dos elementos cualesquiera, sean adyacentes o no, que se encuentran en su orden natural en una permutación constituyen una *permanencia;* dos elementos cualesquiera que se encuentran en un orden que no es su orden natural constituyen una *inversión.* Por ejemplo, la permutación 1, 2 se denomina una permanencia; 2, 1 es una inversión. Dada una permutación *daecb,* y aceptando que el orden alfabético es el orden natural, tenemos permanencias *de, ae, ac, ab,* e inversiones *da, dc, db, ec, eb, cb.* Dada una permutación cualquiera, podemos determinar las permanencias y las inversiones como se hizo anteriormente, considerando el primer elemento con cada uno de los otros elementos; el segundo elemento con cada uno de los elementos que le siguen; el tercer elemento con cada uno de los elementos siguientes, ... De esta manera podemos asociar con cada permutación un entero único no negativo que es el número de inversiones de la permutación. Es así como cualquiera permutación dada puede clasificarse como *par* o *impar* según que el número de inversiones de la permutación sea par o impar. Todas las permutaciones de (v - 4) se encuentran en su orden natural y son permutaciones pares, dado que no tienen inversiones (cero es un número par). Todas las permutaciones de (v - 5) son permutaciones impares, dado que contienen exactamente una inversión. Dado que toda permutación de cualquier conjunto dado de elementos es par o impar, nos referiremos a la *clase* de las permutaciones pares y a la clase de permutaciones impares.

Dada la permutación 4132, podemos considerar las diferencias $1 - 4$, $3 - 4$, $2 - 4$, $3 - 1$, $2 - 1$, $2 - 3$ y encontrar que cuatro de estas diferencias son negativas. La permutación tiene cuatro inversiones y es par. En general, si asociamos un número positivo con cada permanencia y un número negativo con cada inversión, entonces el producto de todos estos números que resultan de una permutación dada es positivo si la permutación es par, y negativo si la permutación es impar. Ya que un entero k precede a un entero m en su orden natural si y sólo si $m - k$ es positivo, un par de números km es una permanencia si $m - k$ es positivo, y es una inversión si $m - k$ es negativo. Por consiguiente, dada una permutación cualquiera de números, podemos considerar el signo del producto R de las diferencias obtenidas al restar cada elemento de la permutación ordenamente de cada uno de los elementos que

le siguen. Por ejemplo, dada la permutación 4132, formamos el producto de las diferencias a que se ha hecho referencia y encontramos que:

$R = (1 - 4)\ (3 - 4)\ (2 - 4)\ (3 - 1)\ (2 - 1)\ (2 - 3)$ es positivo y como se vio anteriormente, la permutación 4132 es par.

Dada la permutación 1432, encontramos que:

$R = (4 - 1)\ (3 - 1)\ (2 - 1)\ (3 - 4)\ (2 - 4)\ (2 - 3)$ es negativo y la permutación 1432 es impar. Esta permutación impar 1432 puede obtenerse de la permutación par 4132, intercambiando los elementos 1 y 4. En general, encontraremos (Teorema V-4) que el intercambio de dos elementos cualesquiera de una permutación (es decir, una *transposición*) cambia la clase de la permutación de par a impar o de impar a par. En la sección siguiente demostraremos el resultado anterior para el caso de transposiciones de elementos adyacentes. También demostraremos que cualquiera permutación de un conjunto dado de elementos puede obtenerse del conjunto de elementos tomado en su orden natural mediante una sucesión de transposiciones de elementos adyacentes.

EJERCICIOS

1. Hacer una lista de las inversiones que hay en las siguientes permutaciones: 7132, 71452, 635421, 192837465.

2. Clasificar cada una de las permutaciones del Ejercicio 1 en pares o impares (a) contando el número de inversiones; (b) teniendo en cuenta el signo del producto de las diferencias R.

3. Indicar la transposición que se ha efectuado en cada una de las tres permutaciones de (v-4) para obtener las permutaciones correspondientes de (v-5).

4. Emplear el símbolo de producto $\prod$ como en el caso especial

$$(x_2 - x_1)(x_3 - x_1)(x_3 - x_2) = \prod_{1 \leqq i < j \leqq 3} (x_j - x_i)$$

y nótese que para la permutación $x_1x_2x_3 \ldots x_n$ se tiene

$$R = \prod_{1 \leqq i < j \leqq n} (x_j - x_i).$$

Este resultado puede escribirse también en la forma

$$R = \prod_{i=1}^{n-1} \prod_{j=2}^{n} (x_j - x_i).$$

V-5 TRANSPOSICIONES. Una transposición (ab) se define como el intercambio de dos elementos cualesquiera a y b en una permutación. En esta sección nos preocuparemos, principalmente, de las transposiciones de elementos adyacentes. Dada la permutación 4132, podemos valernos de la sucesión de transposiciones de elementos adyacentes:

(V - 6) $$(14),\ (23),\ (24),\ (34)$$

para obtener la sucesión de permutaciones:

(V - 7) 4132, 1432, 1423, 1243, 1234,

que comienza con la permutación dada y termina con los elementos en su orden natural. Aunque esto puede hacerse de varias maneras, por conveniencia hemos considerado, simplemente, los números 1, 2, 3, 4 en orden y en la permutación hemos conseguido que cada uno quede en el lugar que le corresponde. En general, dada cualquiera permutación de los elementos $a_1, a_2, a_3, \ldots, a_n$, como

(V - 8) $$a_{j_1}\ a_{j_2}\ a_{j_3}\ \ldots\ a_{j_n},$$

el elemento a_i debe figurar entre los a_{j_k}. Si $a_1 = a_{j_1}$, bastará una sola transposición $(a_{j_1}a_1)$ para colocar a_i en el lugar correspondiente (respecto al orden natural de sus elementos). Si $a_i = a_{j_2}$, pueden hacerse dos transposiciones de elementos adyacentes $(a_{j_2}a_{j_1})$ y $(a_{j_1}a_i)$. En general, si $a_i = a_{j_k}$, se pueden hacer $k-1$ transposiciones de elementos adyacentes. Análogamente, una vez obtenido a_i como el primer elemento, podemos considerar la nueva permutación de la forma:

$$a_i a_{r_1} a_{r_2} \ldots\ a_{r_{n-1}},$$

donde $a_2 = a_{r_s}$, y pueden hacerse $s - 1$ transposiciones de elementos adyacentes para obtener la permutación:

$$a_i a_2 a_{t_1} a_{t_2} \ldots a_{t_{n-2}},$$

Ya que la permutación (v-8) contiene solamente un número finito de elementos, este procedimiento puede continuarse hasta que todos los elementos estén en su orden natural. Estudiaremos, en primer lugar, permutaciones de un número finito de elementos, es decir, *permutaciones finitas*, ya hemos demostrado:

TEOREMA V-1. *Los elementos de cualquiera permutación finita pueden obtenerse en su orden natural por medio de una sucesión finita de transposiciones de elementos adyacentes.*

La sucesión de permutaciones (v-7) resulta al usar la sucesión de transposiciones (v-6) para obtener los elementos de la permutación 4132 en su orden natural. Consideremos ahora el problema de obtener la permutación 4132 del orden natural de sus elementos 1234. Si comenzamos con la permutación 1234, el intercambio de 1 y 4 como se señala en (v-6) no representa una transposición de elementos adyacentes en la permutación. Sin embargo, si se emplea la sucesión de transposiciones:

$$(34),\ (24),\ (23),\ (14),$$

que resulta de considerar la sucesión de transposiciones (v-6) en orden inverso, obtenemos las permutaciones:

$$1234,\ 1243,\ 1423,\ 1432,\ 4132,$$

es decir, la sucesión (v-7) en orden inverso. En general, se tiene

TEOREMA V-2. *Si en una permutación dada se puede emplear una sucesión ordenada S de transposiciones de elementos adyacentes para obtener los elementos de esta permutación en su orden natural, entonces, la sucesión de transposiciones que resulta de emplear las transposiciones de la sucesión S en orden inverso puede aplicarse a la permutación de los elementos en su orden natural con el objeto de obtener la permutación dada.*

La demostración de este teorema es una consecuencia inmediata (Ejercicio 3) de dar por aceptada la sucesión *S*, de admitir la sucesión correspondiente de permutaciones y del hecho de que las transposiciones (ab) y (ba) tienen el mismo efecto en la permutación.

Dada cualquiera permutación (v-8) consideremos el efecto de una transposición de elementos adyacentes $(a_{j_k}a_{j_{k+1}})$ en la clase (par o impar) de la permutación dada. Para cualquier $r < k$ o $r > k + 1$ el orden de a_{j_r} y de a_{j_k} como también el orden de a_{j_r} y de $a_{j_{k+1}}$ no se altera con la transposición. Por consiguiente, el único efecto sobre la clase de la permutación se produce al reemplazar $a_{j_k}a_{j_{k+1}}$ por $a_{j_{k+1}}a_{j_k}$. Este reemplazo introduce una nueva inversión si $a_{j_k}a_{j_{k+1}}$ era

una permanencia, y hace desaparecer una inversión si $a_{j_k}a_{j_{k+1}}$ era una inversión. Por consiguiente, una sola transposición de elementos adyacentes hace variar siempre el número de inversiones en una y se tiene

TEOREMA V-3. *Una sola transposición de dos elementos adyacentes de una permutación cualquiera hace variar la clase de la permutación.*

Los tres teoremas anteriores pueden usarse en varios de los ejercicios siguientes para indicar relaciones entre la clase de una permutación y ciertas sucesiones de transposiciones de sus elementos. En la sección que sigue encontraremos que se verifican relaciones muy análogas cuando los elementos permutados no son necesariamente adyacentes en la permutación.

EJERCICIOS

1. Indicar una sucesión de transposiciones de elementos adyacentes que pueda usarse en cada una de las siguientes permutaciones para colocar los elementos de ellas en su orden natural: 3214, *adcb*, 152634, *ptqsr*.

2. Repetir el Ejercicio 1 para las permutaciones 152634 y *ptqsr*, de varias maneras.

3. Demostrar el Teorema v-2.

4. Proponer por lo menos tres sucesiones diferentes de transposiciones de elementos adyacentes que puedan usarse para obtener la permutación 4132 de 1234.

5. Proponer una sucesión de transposiciones de elementos adyacentes para cada una de las permutaciones del Ejercicio 1 y que puedan usarse para obtener la permutación a partir del orden natural de sus elementos.

6. Repetir de varias maneras el Ejercicio 5 para las permutaciones 152634 y *ptqsr*.

7. Demostrar que para cualquier entero positivo n podemos obtener cualquiera permutación dada de n elementos a partir de la permutación de sus elementos en su orden natural, mediante una sucesión de a lo sumo $n(n-1)/2$ transposiciones de elementos adyacentes.

8. Verificar que cada una de las permutaciones impares de los Ejercicios 1, 2, 4, 5, 6, ha sido permutada hasta obtener el orden natural de sus elementos o se ha obtenido a partir del orden natural de sus elementos mediante un número impar de transposiciones. Repetir este ejercicio para las permutaciones pares.

9. Demostrar que todas las permutacionesde $a_1, a_2, \ldots, a_n$ pueden obtenerse

empleando solamente transposiciones de la forma $(a_j a_n)$, en donde n es fijo y j puede tomar los valores 1, 2, . . . , n-1.

10. ¿Es siempre posible obtener una permutación par a partir del orden natural de sus elementos mediante un número impar de transposiciones de elementos adyacentes? Explicar.

11. Demostrar que para n mayor que 1 son pares exactamente la mitad de las $n!$ permutaciones.

12. Hacer una segunda demostración del Teorema v-3, por medio de R tal como en el Cap. v-4, Ejercicio 4.

V-6 PERMUTACIONES PARES E IMPARES. Hemos visto en el Capítulo v-4 cómo calcular el número de inversiones de cualquiera permutación dada y cómo clasificar la permutación en par o impar, según que el número de inversiones sea par o impar. También hemos visto en el Capítulo v-5 que cualquiera permutación dada puede obtenerse de o transformarse en una permutación de los elementos en su orden natural mediante una sucesión de transposiciones de elementos adyacentes. Dado que cada transposición se asocia (Teorema v-3) en este procedimiento con una sola inversión, toda permutación par puede obtenerse de o transformarse en el orden natural de sus elementos mediante un número par de transposiciones de elementos adyacentes (Teoremas v-1 y v-2). Análogamente, toda permutación impar puede obtenerse de o transformarse en el orden natural de sus elementos mediante un número impar de transposiciones de elementos adyacentes. Demostraremos, ahora, que cualquiera transposición, es decir, cualquier intercambio de dos elementos (adyacentes o no), de una permutación, puede obtenerse mediante un número impar de transposiciones de elementos adyacentes. Por consiguiente, demostraremos que cualquiera transposición de los elementos de una permutación cambia la clase de la permutación.

Dada cualquiera permutación, sabemos que (Teorema v-3) el intercambio de dos elementos adyacentes cambia la clase de la permutación. El intercambio de dos elementos separados por un solo elemento entre ellos, puede efectuarse mediante tres transposiciones de elementos adyacentes. Por ejemplo, las transposiciones:

$$(ab) \quad (ac) \quad (bc)$$

pueden utilizarse para cambiar entre sí los elementos a y c en la permutación abc. La sucesión correspondiente de permutaciones es

$$abc, \quad bac, \quad bca, \quad cba.$$

El intercambio de dos elementos de una permutación que tienen entre sí dos elementos, puede efectuarse mediante cinco transposiciones de elementos adyacentes. Por ejemplo, a y d en $abcd$ pueden cambiarse entre sí por medio de la sucesión de transposiciones:

$$(ab) \quad (ac) \quad (ad) \quad (cd) \quad (bd)$$

que determina la sucesión de permutaciones:

$$abcd, \quad bacd, \quad bcad, \quad bcda, \quad bdca, \quad dbca$$

En general, el intercambio de dos elementos de una permutación que tienen entre sí k elementos puede efectuarse mediante $2k + 1$ transposiciones de elementos adyacentes (Ejercicio 1). De aquí que, de acuerdo con el Teorema v-3, se pueda cambiar la clase de cualquiera permutación por medio de un solo cambio de dos cualesquiera de sus elementos. En otras palabras, hemos demostrado

TEOREMA v-4. *La clase de una permutación cualquiera se cambia por medio de una transposición cualquiera de sus elementos.*

Podemos valernos del producto de las diferencias (Ejercicio 2) tal como en el Ejercicio 4, Capítulo v-4, para hacer una segunda demostración del Teorema v-4. Este teorema se necesitará en el Capítulo v-8 para la demostración de una de las propiedades básicas de los determinantes. Ahora nos apartaremos de nuestra discusión de las propiedades de las permutaciones para estudiar el empleo de las permutaciones en la definición del determinante de una matriz cuadrada.

EJERCICIOS

1. Demostrar que en una permutación se puede efectuar el cambio de dos elementos que tengan entre sí k elementos por medio de $2k + 1$ transposiciones de elementos adyacentes.

2. Empléese el método del Ejercicio 12, Cap. v-5, para proponer una segunda demostración del Teorema v-4.

3. Demostrar que puede obtenerse una permutación cualquiera dada de n

elementos del orden natural de sus elementos por medio de una sucesión de a lo más $n - 1$ transposiciones.

4. En el Teorema v-2, reemplácese "transposición de elementos adyacentes" por "transposición" y demuéstrese el teorema que resulta.

5. Considérense transposiciones arbitrarias de elementos (no necesariamente adyacentes) de la permutación 123 y demuéstrese que la permutación que resulta depende del orden en que se efectúen las transposiciones, es decir, que la aplicación de una sucesión de transposiciones no es necesariamente una operación conmutativa.

6. Valiéndose de las sucesiones de transposiciones (21), (24); (43), (42), (41), (23); (24), (14) y del orden natural 1234, demostrar que la permutación 4132 puede obtenerse del orden natural por medio de varias sucesiones diferentes de transposiciones.

7. Citar por lo menos cuatro sucesiones diferentes de transposiciones que puedan emplearse para obtener la permutación 1234 de 4132.

8. Indicar varios ejemplos de sucesiones de transposiciones que (a) sean conmutativas; (b) no sean conmutativas.

V-7 DETERMINANTES. En esta sección consideraremos un procedimiento explícito para escribir el determinante de cualquiera matriz cuadrada. Como se señaló en el Cap. v-2, el determinante de una matriz cuadrada se define como un polinomio en los elementos de la matriz. Este polinomio puede obtenerse de diferentes maneras. Nos preocuparemos, principalmente, de dos de estos métodos: el desarrollo de un determinante de una matriz cuadrada con respecto a una fila y el desarrollo de un determinante de una matriz cuadrada con respecto a una columna. Estos desarrollos difieren solamente en el método empleado para obtener los términos del polinomio. En el Capítulo v-8 se demostrará que son equivalentes.

Estrictamente hablando, *el desarrollo de un determinante de una matriz cuadrada respecto de una fila* puede definirse como la suma algebraica de todos los productos posibles que se obtienen al tomar uno y sólo un factor de cada fila y columna de la matriz, en donde cada producto se encuentra precedido de un signo más o de un signo menos, según que el número de inversiones de los índices de columna de los factores sea par o impar y en donde los índices de fila se encuentran en su orden natural (ver Bibilografía Nº 16, pág. 3). Consideremos unos cuantos ejemplos de esta definición.

Dada cualquiera matriz cuadrada de dos filas y dos columnas:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \tag{V-9}$$

Podemos designar el determinante de esta matriz por:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \tag{V-10}$$

y buscar el desarrollo del determinante con respecto a la fila. Siendo así (v-10) representa el determinante de (v-9) y (v-9) es la matriz de (v-10). Por definición, el determinante de (v-9) es el polinomio $a_{11}a_{22} - a_{12}a_{21}$.

Conforme a la definición anterior del desarrollo de un determinante con respecto a una fila, podemos elegir cualquier elemento, como ser a_{11}, y tomar junto con él un elemento que no se encuentre en la misma fila ni en la misma columna que a_{11} en la matriz del determinante. En otras palabras, si elegimos a_{11}, tachamos la primera fila y la primera columna.

$$\begin{vmatrix} \cancel{a_{11}} & \cancel{a_{12}} \\ \cancel{a_{21}} & a_{22} \end{vmatrix}$$

y elegimos un elemento de entre los restantes. En el caso de (v-10) queda sólo un elemento, y obtenemos el producto $a_{11}a_{22}$. En general, se repite el procedimiento tachando la fila y la columna del nuevo elemento elegido hasta que quede un solo elemento. Una vez elegido el producto $a_{11}a_{22}$ en (v-9) o en (v-10), queda únicamente otro producto $a_{12}a_{21}$. Cada uno de estos productos puede escribirse de dos maneras: $a_{11}a_{22}$ o bien $a_{22}a_{11}$ y $a_{12}a_{21}$ o bien $a_{21}a_{12}$. Conforme a la definición anterior, tomaremos estos productos en las formas $a_{11}a_{22}$ y $a_{12}a_{21}$ en donde los índices de la fila (los primeros subíndices), se encuentran en su orden natural. En seguida, tomaremos cada producto con un signo más si el índice de la columna (segundo subíndice), forma una permutación par, y con signo menos si el índice de la columna forma una permutación impar. Por consiguiente, el determinante de (v-9) puede expresarse como:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}. \tag{V-11}$$

Si hubiéramos comenzado con un elemento diferente, como ser, a_{21} en vez de a_{11}, habríamos obtenido una expresión equivalente, tal como $-a_{21}a_{12} + a_{22}a_{11}$, del desarrollo del determinante con respecto a la fila.

Antes de considerar otros ejemplos de la definición anterior, vamos a definir el orden de una matriz cuadrada. Se denomina *orden* de una matriz cuadrada su número de filas (o columnas). Por eso (v-9) es una matriz de orden 2 y (v-2) es una matriz de orden n. Análogamente (v-10), representa un determinante de orden 2 y, en general, el orden del determinante de una matriz cuadrada es el mismo que el orden de la matriz.

Hemos aplicado la definición anterior del desarrollo de un determinante con respecto a una fila a determinantes de orden 2. Un determinante de orden 3 puede desarrollarse análogamente (Ejercicio 1) por medio de $3! = 6$ productos de tres factores cada uno de la siguiente manera:

$$\text{(V—12)} \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} - a_{12}a_{21}a_{33} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

El polinomio de (v-11) puede expresarse en la forma

$$\sum e_{j_1 j_2} a_{1 j_1} a_{2 j_2},$$

en donde Σ es el símbolo de la suma, y donde se suma $2! = 2$ permutaciones de los segundos subíndices, y $e_{j_1 j_2}$ se toma como $+1$ o -1, según que la permutación de los segundos subíndices sea par o impar con respecto al orden natural de los enteros positivos. Análogamente, el polinomio de (v-12) puede expresarse en la forma

$$\sum e_{j_1 j_2 j_3} a_{1 j_1} a_{2 j_2} a_{3 j_3},$$

donde se suman las $3! = 6$ permutaciones de los segundos subíndices. En general, el desarrollo del determinante (v-2) de una matriz de orden n con respecto a la fila puede expresarse en la forma

$$\text{(V—13)} \qquad \sum e_{j_1 j_2 \ldots j_n} a_{1 j_1} a_{2 j_2} \ldots a_{n j_n},$$

donde se suman las $n!$ permutaciones de los segundos subíndices y las e son, como anteriormente, $+1$ o -1, según que las permutaciones de los segundos subíndices sean pares o impares. Dado

que este desarrollo general de un determinante de orden n es un polinomio que implica únicamente operaciones de anillo entre los elementos del determinante, podemos esperar encontrar una interpretación a los determinantes y matrices de elementos pertenecientes a cualquier dominio de integridad (véanse los párrafos de la introducción al Capítulo II). Las matrices y determinantes más comunes de las matemáticas elementales tienen por elementos números reales arbitrarios. Supondremos que este es el caso en la mayor parte de este capítulo, pero consideraremos también algunas aplicaciones de matrices cuyos elementos son polinomios. Las matrices cuyos elementos son números complejos desempeñan un papel importante en las teorías de matemáticas superiores.

En la sección siguiente consideraremos tres propiedades de los determinantes que, especialmente en el caso de $n > 3$, suelen permitirnos simplificar el método formal anterior para desarrollar un determinante dado. Para $n = 2$ se obtiene fácilmente el polinomio (v-11) como el producto de los elementos de la diagonal principal (de índices iguales), disminuido en el producto de los elementos de la diagonal secundaria. Para $n = 3$ existe también un método análogo en el que se emplean líneas diagonales. Ya que muchos lectores han empleado previamente el método de (v-14), lo hemos mencionado con el objeto de insistir en que no existe un método análogo para n mayor que 3. Para $n = 3$ se puede copiar nuevamente las dos primeras columnas de la manera siguiente:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{vmatrix} \tag{V-14}$$

y sumar los productos de los elementos sobre las diagonales paralelas a la diagonal principal

$$a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32},$$

y de éstos sustraer la suma de los productos de los elementos sobre las diagonales paralelas a la diagonal secundaria, es decir, sumar los productos negativos

$$-a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}.$$

Sin embargo, este método daría sólo $2n = 8$ términos del polinomio para determinantes de orden 4, en circunstancias en que se necesitan $n! = 24$ términos. En general, el método anterior de las

diagonales (v-14) puede utilizarse solamente para determinantes de orden menor o igual a 3. Para determinantes de todos los órdenes pueden usarse otros métodos más adecuados (Cap. v-9 y Cap. v-10) y se recomiendan en lugar de aquel de (v-14) para determinantes de orden 3.

EJERCICIOS

1. Obtener el desarrollo de un determinante (v-12), con respecto a la fila, valiéndose de la definición formal del mismo.

2. Encontrar el desarrollo con respecto a la fila de

$$\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \text{ y de } \begin{vmatrix} 2 & 3 \\ 4 & 6 \end{vmatrix}.$$

3. Encontrar el desarrollo con respecto a la fila de

$$\begin{vmatrix} 1 & 2 & 3 \\ 1 & 0 & 1 \\ 2 & 1 & 2 \end{vmatrix}.$$

4. Encontrar el desarrollo con respecto a la fila de

$$\begin{vmatrix} 2 & 1 & 5 \\ 3 & -2 & 2 \\ 1 & -1 & 0 \end{vmatrix}.$$

5. Escribir una matriz general de orden 4 por medio de (v-2) haciendo $n = 4$. Encontrar el desarrollo del determinante de esta matriz con respecto a la fila.

6. Encontrar y simplificar el desarrollo con respecto a la fila de

$$\begin{vmatrix} 1 & 2 & 3 & 1 \\ 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{vmatrix}.$$

7. Definir el desarrollo del determinante de una matriz cuadrada con respecto a la columna cambiando la palabra "fila" por "columna" en la definición del desarrollo de un determinante con respecto a la fila.

8. Repetir el Ejercicio 2, haciendo el desarrollo con respecto a la columna.

9. Encontrar el desarrollo del determinante de (v-9) con respecto a la columna y compararlo con el desarrollo con respecto a la fila.

10. Encontrar el desarrollo de (v-12) con respecto a la columna y compararlo con el desarrollo con respecto a la fila.

11. Repetir los Ejercicios 3 y 4, haciendo el desarrollo con respecto a la columna.

12. Encontrar el desarrollo de una matriz general de orden 4 con respecto

a la columna y compararlo con el desarrollo con respecto a la fila que se obtuvo en el Ejercicio 5.

13. Repetir el Ejercicio 6, haciendo el desarrollo con respecto a la columna.

14. Expresar los desarrollos de matrices cuadradas de orden 2, 3, 4, y n con respecto a la columna, valiéndose de la notación para la suma como en (v-13).

V-8 PROPIEDADES DE LOS DETERMINANTES. En esta sección emplearemos los desarrollos con respecto a la fila

(V-15) $$a_{11}a_{22} - a_{12}a_{21}$$

(V-16) $$a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32}$$

para los determinantes (v-11) y (v-12) de matrices generales de segundo y tercer orden para ilustrar tres propiedades básicas de los determinantes. Emplearemos la palabra *línea* de una matriz para indicar indistintamente una fila o una columna. Esta notación es muy útil para el caso en que una proposición se aplique por igual a filas y columnas.

Cada término del polinomio (v-15) tiene exactamente un factor con el primer subíndice 1, es decir, cada término tiene exactamente un factor que pertenece a la primera fila de la matriz del determinante. Análogamente, cada término tiene exactamente un factor de la segunda fila, de la primera columna, de la segunda columna. En consecuencia, cada término del desarrollo con respecto a la fila (v-15) tiene exactamente un factor de cada línea de la matriz del determinante (v-11). En otras palabras, el desarrollo con respecto a la fila (v-15) es lineal y homogéneo en los elementos de cada línea de la matriz del determinante.

Esto mismo se puede afirmar con respecto al desarrollo (v-16) del determinante (v-12) con respecto a la fila. Cada término del desarrollo con respecto a la fila contiene exactamente un factor perteneciente a cada línea de la matriz del determinante, es decir, el desarrollo con respecto a la fila es lineal y homogéneo en los elementos de cada línea de la matriz del determinante. Nuestra primera propiedad básica de los determinantes resulta al expresar esto mismo para determinantes de cualquier orden n.

PROPIEDAD A. *El desarrollo de un determinante con respecto a la fila es lineal y homogéneo en los elementos de cada línea de su matriz.*

Utilizaremos, en seguida, esta propiedad y consideraremos unos cuantos métodos particulares de desarrollar el determinante general de tercer orden (v-12). Si en el determinante (v-16) reunimos los coeficientes de los elementos de la primera fila del determinante, tenemos:

$$(V\text{-}17)\quad a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}),$$

en donde se ha sumado el término que contiene a_{1j} si $1 + j$ es par y se ha restado si $1 + j$ es impar. La importancia de esta convención se apreciará luego al estudiar determinantes menores de elementos.

El desarrollo (v-17) se denomina un desarrollo respecto de los elementos de la primera fila de la matriz del determinante. Análogamente, el determinante general de tercer orden puede desarrollarse respecto de los elementos de cualquiera línea de la matriz del determinante (Ejercicio 1).

Si los elementos de la primera fila de la matriz de (v-12) son todos cero, es decir, $a_{11} = a_{12} = a_{13} = 0$, entonces el desarrollo (v-17) es cero. Ya que cualquier determinante puede expresarse por medio de los elementos de cualquiera línea de la matriz del determinante, valiéndonos de la Propiedad A, tenemos

TEOREMA V-5. *Si todos los elementos de una línea de una matriz cuadrada son iguales a cero, su determinante es cero.*

Volviendo a (v-17) veremos que el coeficiente de a_{11} es precisamente el desarrollo del determinante que se obtiene tachando en (v-12) la fila y la columna correspondiente a a_{11}. Lo mismo ocurre para a_{12} y, con excepción del signo, para a_{13}. En general, denominaremos *el menor de un elemento* de una matriz cuadrada de orden n, al determinante de orden $n - 1$ que se obtiene tachando la fila y la columna correspondiente al elemento. En seguida denominaremos *cofactor* A_{ij} de un elemento a_{ij} al coeficiente de a_{ij} en el determinante (v-13). Ya hemos observado que los cofacto-

res de a_{11} y de a_{13} en (v - 17) son iguales a sus menores, en circunstancias de que el cofactor de a_{12} es el negativo del menor de aquel elemento. De acuerdo con la Propiedad C y con (v - 13) podemos probar en el Ejercicio 15 de esta sección y mediante otro método en el Ejercicio 4, Capítulo v - 10, que el cofactor de cualquier elemento a_{ij} es $(-1)^{i+j}$ veces el menor de a_{ij}.

Valiéndonos de la definición anterior de cofactor, el desarrollo de un determinante de orden n puede expresarse:

$$a_{11}A_{11} + a_{12}A_{12} + \quad \cdot + a_{1n}A_{1n}$$

por medio de los menores de los elementos de la primera fila de la matriz del determinante, o también por medio de los menores de los elementos de la fila i-ésima,

(V -18) $\qquad a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{in}A_{in}$, o también

(V - 19) $\qquad a_{1j}A_{1j} + a_{2j}A_{2j} + \ldots + a_{nj}A_{nj}$

por medio de los menores de los elementos de la columna j-ésima. Es costumbre hablar del desarrollo de un determinante por medio de los menores de sus elementos en la forma que se acaba de señalar, en lugar de hablar de cofactores para referirse a los menores tomados con el signo que les corresponde. El Teorema v - 5 pudo haberse postergado para introducirse aquí como consecuencia inmediata de estos desarrollos.

Si cada elemento de la primera fila de la matriz (v - 12) se multiplica por k, entonces a_{11}, a_{12}, a_{13} de (v - 17) se reemplazan por ka_{11}, ka_{12}, ka_{13} y el determinante de la matriz ha quedado multiplicado por k. De la misma manera, de (v - 18) y de (v - 19), se obtiene

TEOREMA v - 6. *Si los elementos de cualquier línea de una matriz se multiplican por k, entonces su determinante queda multiplicado por k.*

Este teorema nos asigna el derecho de sacar un factor común de cualquiera línea de la matriz de un determinante y de multiplicarlo por el determinante de la nueva matriz. Por ejemplo, se tiene

$$\begin{vmatrix} 4 & 6 \\ 1 & 3 \end{vmatrix} = 2\begin{vmatrix} 2 & 3 \\ 1 & 3 \end{vmatrix} = 6\begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} = 6.$$

El Teorema v - 6 puede demostrarse también directamente del desarrollo (v - 13) y de la Propiedad A (Ejercicio 8).

Las otras dos propiedades básicas de los determinantes pueden ilustrarse, respectivamente, mediante el intercambio de filas y columnas en la matriz de un determinante

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{vmatrix}$$

y mediante el intercambio de dos filas de la matriz de un determinante, cambiando el signo del determinante:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = -\begin{vmatrix} a_{21} & a_{22} \\ a_{11} & a_{12} \end{vmatrix}.$$

Estas propiedades constituirán la base de los procedimientos para simplificar el desarrollo de un determinante (Cap. v - 9). El término identidad se define en el Cap. III - 4 en el sentido en que se usa en el siguiente enunciado:

PROPIEDAD B. *El desarrollo de un determinante de una matriz cuadrada con respecto a una fila es idéntico al desarrollo del determinante respecto de una columna.*

PROPIEDAD C. *El intercambio de dos líneas paralelas cualesquiera en una matriz cuadrada, cambia el signo de su determinante.*

Estas dos propiedades pueden demostrarse por medio del desarrollo (v - 13). El término "dos líneas paralelas" se refiere a dos filas o a dos columnas. La propiedad B establece que

$$\sum e_{i_1 i_2 \cdots i_n} a_{1 j_1} a_{2 j_2} \cdots a_{n j_n} = \sum e_{k_1 k_2 \cdots k_n} a_{k_1 1} a_{k_2 2} \cdots a_{k_n n},$$

en donde se han sumado las $n!$ permutaciones de los índices de fila y columna respectivamente. Las dos sumas contienen cada una todos los $n!$ productos posibles de los elementos a_{ij} de tal manera

que ningún par de elementos sea de la misma fila ni tampoco ningún par de elementos sea de la misma columna. Por consiguiente, sólo queda por demostrar que cada producto (término de la suma) tiene el mismo signo cuando sus factores están ordenados respecto de sus índices de fila que cuando están ordenados respecto de sus índices de columna. Por ejemplo, cuando $n = 3$, tenemos un término $a_{12}a_{23}a_{31}$. Si se ha ordenado respecto de los índices de fila, la permutación de los índices de columna es 231, que puede obtenerse del orden natural por la sucesión de transposiciones (12), (13) y por lo tanto es par. Si se ordena respecto de los índices de columna, tenemos $a_{31}a_{12}a_{23}$ y la permutación de los índices de fila es 312, que puede obtenerse del orden natural por medio de (23), (13) y por lo tanto es también par. De aquí que el término $a_{12}a_{23}a_{31}$ en el desarrollo de un determinante de tercer orden sea positivo, ya sea que el determinante se haya desarrollado respecto de las filas o respecto de las columnas. Esto es verdadero esencialmente (ver Teorema v - 2), porque la misma sucesión (12), (13) de transposiciones empleadas para obtener la permutación 231 de los índices de columna a partir de su orden natural puede también usarse en orden inverso (13), (12), en la permutación 231 para ordenar los índices de columna en su orden natural y obtener de este modo $a_{31}a_{12}a_{23}$. En general, la sucesión de transposiciones que se emplea para obtener la permutación de los índices de columna de $a_{1j_1}\ a_{2j_2}\ \ldots\ a_{nj_n}$ a partir de su orden natural, puede usarse en orden inverso para ordenar los factores conforme a sus índices de columna $a_{k_11}\ a_{k_22}\ \ldots\ a_{k_nn}$. Dado que las dos sucesiones de transposiciones contienen el mismo número de transposiciones, las dos permutaciones son ambas pares o ambas impares y por lo tanto, cada término del desarrollo del determinante tiene el mismo signo ya sea que el determinante se haya desarrollado por filas o por columnas. Con esto se completa la demostración de la Propiedad B y se justifica la equivalencia entre los desarrollos (v - 18) y (v - 19).

La Propiedad C puede demostrarse rápidamente valiéndose del Teorema v - 4 de la manera siguiente: Si se cambian dos columnas de una matriz, cada permutación de (v - 13) cambia de clase y cada término del desarrollo cambia de signo. Para obtener el mismo resultado cuando se cambian dos filas cualesquiera se puede aprovechar la Propiedad B y el desarrollo por columnas.

El teorema siguiente es una consecuencia inmediata (Ejercicio 12) de la Propiedad C y del Teorema v - 6.

TEOREMA V - 7. *Si en una matriz cuadrada dos líneas paralelas son proporcionales, su determinante es igual a cero.*

En las dos secciones siguientes, utilizaremos las propiedades y teoremas anteriores para exponer métodos que simplifiquen la tarea de desarrollar el determinante de cualquiera matriz cuadrada dada.

EJERCICIOS

1. Valiéndose de (v-16) proponer desarrollos análogos a (v-17) de (v-12) respecto de los elementos de (a) su segunda fila; (b) su tercera fila; (c) su primera columna; (d) su tercera columna.

2. Proponer una matriz cuadrada de orden 3 que ilustre el Teorema v-5.

3. Dar un ejemplo de una matriz cuadrada de orden 2 con determinante cero y elementos diferentes de cero.

4. Indicar el determinante menor de cada elemento de (v-12).

5. Indicar el cofactor de cada elemento de (v-12).

6. Repetir el Ejercicio 1, empleando cofactores.

7. Indicar los cofactores de cada elemento del determinante de una matriz general de orden 4.

8. Demostrar el Teorema v-6 directamente de (v-13) y de la Propiedad A.

9. Valiéndose del Teorema v-6, escribir los siguientes determinantes como productos de fracciones y determinantes con elementos enteros:

$$\begin{vmatrix} \frac{1}{2} & \frac{1}{3} \\ \frac{1}{4} & \frac{1}{6} \end{vmatrix}, \quad \begin{vmatrix} 1 & \frac{1}{2} & \frac{1}{4} \\ 2 & 3 & 5 \\ 2 & \frac{2}{3} & -1 \end{vmatrix}.$$

10. Demostrar que el determinante de cualquiera matriz cuadrada que tiene los elementos de una línea respectivamente proporcionales a los elementos correspondientes de una línea paralela a ella, puede expresarse como un múltiplo constante del determinante de una matriz que tiene dos líneas paralelas idénticas.

11. Demostrar que una matriz que tiene dos líneas paralelas idénticas tiene determinante igual a cero.

12. Demostrar el Teorema v-7.

13. Demostrar que el cofactor de a_{11} es igual a su menor.

14. Demostrar que el cofactor de a_{ij} es $(-1)^{i+j}$ veces su determinante menor.

15. Demostrar que el cofactor de a_{ij} es $(-1)^{i+j}$ veces su determinante menor.

16. Dado el determinante siguiente:

$$\begin{vmatrix} 3 & 1 & 2 & 5 \\ 4 & -1 & 3 & 1 \\ 6 & 2 & 4 & 3 \\ -1 & 1 & 1 & 2 \end{vmatrix}$$

escribirlo nuevamente de modo que sus elementos sean enteros y que todos los elementos de la primera columna sean iguales a $+1$.

17. Demostrar que

$$\begin{vmatrix} yz & 1 & x \\ zx & 1 & y \\ xy & 1 & z \end{vmatrix} = \begin{vmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{vmatrix}.$$

18. Demostrar que $a_{1j}A_{1k} + a_{2j}A_{2k} + \cdots + a_{nj}A_{nk} = 0$ y que cuando $j \neq k$. $a_{j1}A_{k1} + a_{j2}A_{k2} + \cdots + a_{jn}A_{kn} = 0$

V-9 DESARROLLO DE LOS DETERMINANTES. Hemos definido explícitamente el desarrollo de un determinante (Cap. v - 7) respecto de la fila y estudiado sus propiedades básicas (Cap. v - 8). Hemos definido (Ejercicio 7, Cap. v - 7) el desarrollo de un determinante respecto de una columna y demostrado que es idéntico con el desarrollo respecto de la fila (Propiedad C, Cap. v - 8). Los desarrollos de un determinante de una matriz cuadrada por medio de determinantes menores de los elementos de una fila dada (v - 18) o de una columna dada (v - 19) son también idénticos con el desarrollo de un determinante respecto de una fila. Por consiguiente, podemos hablar de *el desarrollo* de un determinante y buscar modos de reducir el trabajo de desarrollar un determinante, es decir, de encontrar el polinomio asociado con cualquiera matriz cuadrada dada. Frecuentemente designaremos determinantes por esquemas tales como (v - 20) con el objeto de tener presente las filas y columnas de la matriz del determinante.

El desarrollo de un determinante de orden n, respecto de una fila tiene $n!$ términos,, en circunstancias de que el desarrollo de un

determinante de orden $n - 1$ respecto de una fila tiene solamente $(n - 1)!$ términos. Por eso, consideraremos métodos para reemplazar un determinante de orden n por un determinante de orden $n - 1$, cambiando solamente la forma del desarrollo y no su valor, es decir, el desarrollo del nuevo determinante de orden $(n - 1)$ debe ser idénticamente igual a aquel del determinante dado de orden n. Por jemplo, si todos los elementos de una línea, con la excepción de uno de ellos, de la matriz de un determinante de orden n son iguales a cero, este determinante puede reemplazarse por un determinante de orden $n - 1$ mediante los desarrollos (v - 18), (v - 19). Para $n = 3$, tenemos las relaciones

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

para elementos arbitrarios a_{ij}. En esta sección consideraremos dos teoremas que nos permitirán emplear los procedimientos mencionados para el determinante de cualquiera matriz cuadrada.

El determinante que se designa por

$$\text{(V - 20)} \qquad \begin{vmatrix} a_{11} + b_{11} & a_{12} + b_{12} & a_{13} + b_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

puede desarrollarse (v - 17) respecto de los elementos de la primera fila de su matriz como sigue:

$$(a_{11} + b_{11})(a_{22}a_{33} - a_{23}a_{32}) - (a_{12} + b_{12})(a_{21}a_{33} - a_{23}a_{31}) + (a_{13} + b_{13})(a_{21}a_{32} - a_{22}a_{31}).$$

Este desarrollo puede escribirse también en la forma

$$a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}) + b_{11}(a_{22}a_{33} - a_{23}a_{32}) - b_{12}(a_{21}a_{33} - a_{23}a_{31}) + b_{13}(a_{21}a_{32} - a_{22}a_{31}),$$

el que, si se compara con (v - 17), se ve que representa la suma de dos determinantes. Esta suma puede designarse por

$$\text{(V - 21)} \qquad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} b_{11} & b_{12} & b_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}.$$

En general, podemos usar el procedimiento citado y demostrar (Ejercicio 1).

TEOREMA v - 8. *Si la j-ésima fila (o columna) de una matriz M está formada por elementos de la forma* $a_{jt} + b_{jt}$, *entonces el determinante D de M satisface* $D = D_1 + D_2$, *en donde* D_1 *y* D_2 *son determinantes de matrices cuyos elementos son los mismos de los de M con la excepción de sus filas j-ésimas (o columnas) que son, respectivamente, los elementos* a_{jt} *y los* b_{jt}.

Si $b_{jt} = ka_{it}$, $t \neq j$, el Teorema v - 8 tiene una aplicación muy útil. Por ejemplo, si $b_{jt} = ka_{it}$ en (v - 20), entonces (v - 21) resulta igual a

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} ka_{21} & ka_{22} & ka_{23} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix},$$

en donde el segundo determinante es cero, conforme al Teorema v - 7. Análogamente, cualquier determinante de tercer orden permanece invariable si se suma a cada elemento de la primera fila un múltiplo constante fijo (positivo o negativo) del elemento correspondiente de la tercera fila de su matriz. También podemos demostrar que un múltiplo constante fijo de los elementos de cualquiera fila de la matriz de un determinante de tercer orden puede sumarse a los elementos correspondientes de cualquier otra fila sin que el determinante varíe. Lo mismo se puede afirmar respecto de las columnas de la matriz de un determinante de tercer orden (Ejercicio 4) y, en general (Ejercicio 5), para filas y columnas de la matriz de cualquier determinante valiéndose de (v - 18) y de (v - 19). Por consiguiente, tenemos:

TEOREMA v - 9. *El determinante de cualquiera matriz cuadrada permanece invariable si se suma a los elementos de cualquiera línea de la matriz, un múltiplo constante fijo de los elementos correspondientes de cualquiera línea paralela distinta.*

Al aplicar el Teorema v - 9, hay que tomar dos precauciones. Primera, no se puede sumar k veces los elementos de una línea a los elementos de la misma línea, ya que esto multiplicaría el determinante por $k + 1$ (Teorema v - 6). Segundo, los nuevos elementos, como $a_{ij} + ka_{ij}$, deben reemplazar a los elementos a_{ij}. Si se usaran para reemplazar a los elementos a_{ij}, el determinante que-

daría, en efecto, multiplicado por k. Tomadas estas precauciones, el Teorema v - 9 es extremadamente útil para cambiar de forma a un determinante, de modo que a lo sumo uno de los elementos de alguna línea de su matriz sea diferente de cero. Luego (v - 18) o (v - 19) pueden usarse para expresar el determinante dado como un número constante de veces un determinante de orden inferior. si $a_{11} = 1$, entonces puede sustraerse a_{i1} veces cada elemento de la primera fila de la matriz del determinante del elemento correspondiente de la segunda fila, y de este modo a_{i1} puede reemplazarse por cero. Análogamente, con la excepción de a_{11}, cada elemento de la primera fila y cada elemento de la primera columna pueden reemplazarse por cero (Ejercicio 7). Si algún a_{ij} satisface $|a_{ij}| = 1$ en cualquier determinante, entonces uno por medio de los elementos de la fila i-ésima y uno por medio de los elementos de la columna j-ésima pueden reemplazarse por cero. En general, el determinante de cualquiera matriz cuadrada cuyos elementos son números reales arbitrarios puede expresarse como el determinante de una matriz que tenga a lo sumo un elemento diferente de cero en cada fila y en cada columna (Ejercicio 16).

El determinante

$$\text{(V - 22)} \qquad \begin{vmatrix} 2 & 5 & 7 \\ 4 & 3 & 2 \\ 2 & 4 & 5 \end{vmatrix}$$

puede desarrollarse, por medio de los principios citados, como sigue: se puede sacar factor común 2 a la primera columna de la matriz del determinante y multiplicar por 2 el determinante de la nueva matriz (Teorema v - 6), a la segunda fila se le puede sustraer el doble de la tercera fila (Teorema v - 9), y a la primera fila se le puede sustraer la tercera. Efectuando estos pasos en el orden establecido, tenemos lo siguiente:

$$2\begin{vmatrix} 1 & 5 & 7 \\ 2 & 3 & 2 \\ 1 & 4 & 5 \end{vmatrix} = 2\begin{vmatrix} 1 & 5 & 7 \\ 0 & -5 & -8 \\ 1 & 4 & 5 \end{vmatrix} = 2\begin{vmatrix} 0 & 1 & 2 \\ 0 & -5 & -8 \\ 1 & 4 & 5 \end{vmatrix}.$$

En seguida desarrollamos el determinante último por medio de los menores de los elementos de la primera columna de su matriz, como en (v - 19), y obtenemos

$$2 \cdot 1\begin{vmatrix} 1 & 2 \\ -5 & -8 \end{vmatrix} = 2(-8 + 10) = 4.$$

Hemos empleado la terminología corriente "desarrollo de un determinante" para designar el procedimiento mediante el cual se obtiene el polinomio o número (es decir, el determinante) asociado con cualquiera matriz cuadrada. Se suele denominar *evaluación* del determinante a su desarrollo cuando los elementos de la matriz son números. En este sentido hemos evaluado el determinante designado por (v - 22) y hemos encontrado que tiene un valor 4, es decir, el determinante es el polinomio 4.

Dado cualquier conjunto de elemento $b_1, b_2, \ldots b_k$, podemos definir a

$$c_1b_1 + c_2b_2 + \ldots + c_kb_k,$$

como una *combinación lineal* de los b, en que los c son constantes y por lo menos un $c_i \neq 0$. Luego el Teorema v - 9 puede ampliarse (Ejercicio 20) y formularse así: El determinante de cualquiera matriz cuadrada permanece invariable si se suman a los elementos de cualquiera línea de la matriz, cualquiera combinación fija lineal de los elementos correspondientes de las otras líneas paralelas. Se dará un ejemplo de este concepto y se insistirá más sobre él en el Capítulo v - 13 al tratar la dependencia lineal.

Ahora podemos desarrollar determinantes de matrices cuadradas de orden n, siendo n cualquier entero positivo, por medio de determinantes menores de los elementos de cualquiera línea. El Teorema v - 9 puede aplicarse para reducir el número de términos del desarrollo. Por eso, es a menudo ventajoso desarrollar un determinante de orden n por medio de determinantes de orden $k < n$ que contengan elementos del determinante dado. Si $k = n - 1$, este desarrollo está indicado en (v - 18) y en (v - 19). En el Capítulo v - 10 consideraremos nuevos métodos para el caso en que $k < n - 1$.

EJERCICIOS

1. Demostrar el Teorema v-8.

2. Dar un ejemplo del Teorema v-8 y comprobarlo, por medio de determinantes de orden 2, con elementos numéricos.

3. Repetir el Ejercicio 2 para determinantes de orden 3.

4. Demostrar que los elementos de cualquier columna de una matriz de tercer orden pueden aumentarse o disminuirse en un múltiplo fijo constante de los elementos correspondientes de cualquier otra columna sin que varíe el determinante de la matriz.

5. Demostrar el Teorema v-9.

6. Dar un ejemplo del Teorema v-9, valiéndose de un determinante de orden 3.

7. Escribir un determinante de tercer orden que tenga $a_{12} = -1$ y $|a_{ij}| > 1$ en el caso en que $a_{11} \neq a_{22}$. Por medio del Teorema v-9, volver a escribir este determinante de modo que a_{21}, a_{23}, a_{13}, y a_{31} se reemplacen por cero.

8. Repetir el Ejercicio 7 para un determinante de orden 4, reemplazando por cero los elementos a_{11}, a_{12}, a_{24}, a_{34}, a_{43} y a_{44}.

9. Evaluar los determinantes

$$\begin{vmatrix} 1 & 2 & 3 \\ 1 & 4 & 3 \\ 1 & 5 & 4 \end{vmatrix}, \quad \begin{vmatrix} 2 & 4 & 6 \\ 1 & 4 & 5 \\ 1 & 2 & 3 \end{vmatrix}, \quad \begin{vmatrix} 2 & 5 & 7 \\ 3 & 5 & 6 \\ 7 & 6 & 5 \end{vmatrix}.$$

[Respuestas: $+2, 0, -6$.]

10. Desarrollar

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & c & 1 & 0 \\ d & e & f & 1 \end{vmatrix}$$

11. Formular y demostrar un teorema general para el desarrollo de determinantes de matrices triangulares como aquella del Ejercicio 10, en la que todos los elementos que se encuentran arriba de la diagonal principal son iguales a cero.

12. Evaluar

$$\begin{vmatrix} 2 & 7 & 5 & 6 \\ 1 & 6 & 4 & 5 \\ 2 & 3 & 4 & 2 \\ 3 & 2 & 1 & 4 \end{vmatrix}.$$

13. Desarrollar los determinantes

$$\begin{vmatrix} x & y & z & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} x & y & z & 1 \\ 1 & 1 & 1 & 1 \\ 2 & 3 & 4 & 1 \\ -1 & 2 & 5 & 1 \end{vmatrix}.$$

14. Por medio del Algoritmo de Euclides (Cap. II-5) demostrar que cualquier determinante de segundo orden (v-10) con elementos enteros puede escribirse reemplazando los elementos a_{12} y a_{21} por cero; es decir, cualquier determinante de segundo orden con elementos enteros puede escribirse de modo que a lo sumo los elementos de la diagonal principal sean diferentes de cero. (Es suficiente usar enteros o, en general, elementos de un dominio de integridad).

15. Demostrar que si en el determinante de tercer orden (v-12) los elementos son números reales, éste puede escribirse de modo que a lo sumo los elementos de la diagonal principal sean diferentes de cero.

16. Señalar un procedimiento por medio del cual el determinante de cualquiera matriz cuadrada cuyos elementos sean números reales arbitrarios, pueda expresarse como el determinante de una matriz tal que tenga a lo sumo los elementos de la diagonal principal de la nueva matriz, diferentes de cero. ¿Sirve el procedimiento dado para el caso en que los elementos del determinante sean elementos arbitrarios de cualquier dominio de integridad dado en el sistema de números complejos?

17. Evaluar

$$\begin{vmatrix} 1 & 2 & 1 & 3 & 1 \\ 2 & 1 & 3 & 2 & 2 \\ 1 & 1 & 4 & 2 & 1 \\ 3 & 4 & 1 & 2 & 2 \\ 2 & 4 & 2 & 4 & 2 \end{vmatrix}.$$

[Respuesta: + 16.]

18. Expresar el siguiente determinante como suma de dos determinantes de tercer orden:

$$\begin{vmatrix} x+a & y+b & z+c \\ 1 & 2 & 3 \\ 4 & 1 & 2 \end{vmatrix}.$$

19. Expresar la suma siguiente de dos determinantes como un solo determinante de tercer orden:

$$\begin{vmatrix} 5 & -6 & 7 \\ 1 & 2 & 3 \\ 1 & 1 & 1 \end{vmatrix} + \begin{vmatrix} 10 & 7 & -5 \\ 1 & 2 & 3 \\ 1 & 1 & 1 \end{vmatrix}$$

20. Demostrar que se puede sumar a los elementos de cualquiera línea de una matriz cuadrada, cualquiera combinación lineal fija de los elementos correspondientes de las otras filas paralelas, sin que varíe el determinante de la matriz.

21. Demostrar que

$$\begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} = (x_3 - x_1)(x_2 - x_1)(x_3 - x_2).$$

22. Ampliar el Ejercicio 21 para demostrar que para cualquier entero k, el determinante de Vandermonde

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{k-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & x_k & x_k^2 & \dots & x_k^{k-1} \end{vmatrix}$$

$$= (x_k - x_1)(x_k - x_2) \dots (x_k - x_{k-1})$$
$$(x_{k-1} - x_1)(x_{k-1} - x_2) \dots (x_{k-1} - x_{k-2})$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$(x_3 - x_1)(x_3 - x_2)$$
$$(x_2 - x_1).$$

V·10 DETERMINANTES MENORES. Hemos establecido una ordenación cuadrada tal como (v · 2) una matriz cuadrada, hemos asociado un determinante con cada matriz cuadrada y definido (Cap. v - 8) el menor de un elemento de una matriz de orden n como el determinante de orden $n - 1$ que se obtiene tachando la fila y la columna correspondientes al elemento. Ampliaremos esta definición como sigue: Dada cualquiera matriz de orden n, la matriz que se obtiene tachando r filas cualesquiera y r columnas cualesquiera de la matriz dada ($r < n$) tiene un determinante de orden $n - r$ que se llama el menor de orden r-ésimo de la matriz dada. Por eso, el menor de cualquier elemento a_{ij} de una matriz es el primer menor de la matriz. El determinante que resulta en (v - 23) tachando la primera y segunda columnas, la segunda y cuarta filas es

$$\text{(V - 23)} \qquad \begin{vmatrix} \cancel{a_{11}} & \cancel{a_{12}} & a_{13} & \cancel{a_{14}} \\ \cancel{a_{21}} & \cancel{a_{22}} & \cancel{a_{23}} & \cancel{a_{24}} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ \cancel{a_{41}} & \cancel{a_{42}} & \cancel{a_{43}} & \cancel{a_{44}} \end{vmatrix} = \begin{vmatrix} a_{13} & a_{14} \\ a_{33} & a_{34} \end{vmatrix}$$

y se denomina el segundo menor de la matriz dada de cuarto orden.

Dada una matriz de orden n, podemos obtener un menor r-ésimo ya sea tachando r filas y r columnas o eligiendo en su orden natural $n - r$ filas y $n - r$ columnas con cuyos elementos se formará el determinante menor en cuestión. Por ejemplo, el menor de a_{11} en una matriz de tercer orden puede obtenerse tachando la primera fila y la primera columna o eligiendo los elementos que se encuentran en la segunda o tercera filas y en la segunda o tercera columnas. Por esos, al contar los primeros menores de una matriz

de tercer orden, podemos decir que hay un menor asociado con cada uno de los 3^2 elementos de la matriz, o bien podemos calcular $C^3_2 = (3 \cdot 2)/2 = 3$ el número de maneras de elegir dos filas de entre tres y también el número de maneras de elegir dos columnas de entre tres, de donde, lo mismo que anteriormente, resultan $(C^3_2)^2 = 9$ menores primeros de una matriz de tercer orden. En general (Ejercicio 1), hay $(C^n_{n-r})^2$ menores r-ésimos de una matriz de orden n-ésimo, en que $C^n_{n-r} = n!/[(n-r)!r!]$ y $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.

Cuando las filas y columnas que se han empleado en formar un menor M_r son precisamente aquellas que sobraron al formar un menor $M_{r'}$ los dos menores $M_{r'}$ y M_r se denominan *menores complementarios*. Por ejemplo,

$$\begin{vmatrix} a_{21} & a_{22} \\ a_{41} & a_{42} \end{vmatrix} \quad \text{y} \quad \begin{vmatrix} a_{13} & a_{14} \\ a_{33} & a_{34} \end{vmatrix}$$

son menores complementarios de la matriz de (v - 23). El *complemento algebraico* de un menor de una matriz es igual a su menor complementario multiplicado por $(-1)^p$, en que p es la suma de los índices de las filas y columnas empleadas en la formación del menor (Ejercicios 3-6 y Bibliografía Nº 9; págs. 23-24). Dado que la suma de todos los índices de fila y de columna de cualquiera matriz cuadrada de orden n es un número par $n(n+1)$, podemos elegir en cambio a p como la suma de los índices de las filas y columnas tachadas. Por consiguiente, el complemento algebraico de un menor corresponde al cofactor de un elemento. En particular, dado que un menor de orden $(n-1)$ es un solo elemento, el complemento algebraico de cualquier elemento de una matriz es su cofactor.

El determinante de cualquiera matriz puede obtenerse eligiendo cualquiera fila de la matriz, multiplicando todos los elementos de esa fila por su complemento algebraico, y efectuando la suma de estos productos, como en (v - 18). Este procedimiento puede también usarse respecto de cualquiera columna de la matriz, como en (v - 19). Estos desarrollos por medio de menores de orden $(n-1)$

de todos los elementos de una línea de la matriz son casos especiales del siguiente teorema:

TEOREMA V - 10. DESARROLLO DE LAPLACE. *Si se seleccionan r líneas paralelas cualesquiera de una matriz M y se forman todos los menores correspondientes a los elementos de las r líneas paralelas, el determinante de M es igual a la suma de los productos de estos menores por su complemento algebraico.*

Esbozaremos la demostración del Teorema v - 10, dejando la mayoría de los detalles para que el lector los complete como ejercicio (Ejercicio 20) o valiéndose de un texto más detallado sobre matrices y determinantes, tal como el Nº 16 de la Bibliografía; págs. 20-22. En resumen, hay que demostrar que cada término del determinante se presenta exactamente una vez con el signo adecuado en el desarrollo de Laplace y que no figuran otros términos. Los términos del desarrollo respecto de una fila de un determinante (Cap. v - 7) son los productos que se obtienen tomando un factor y sólo uno de cada fila y columna de la matriz del determinante. En consecuencia, cada término del determinante de una matriz de orden n tiene n factores. Supondremos que los elementos de la matriz pertenecen a un anillo en el que la multiplicación es conmutativa. Luego los $n!$ términos del determinante son independientes de las permutaciones de las filas y columnas, es decir, se puede demostrar que cada término aparece una y sólo una vez, sea que el desarrollo se haya efectuado por medio de los menores de orden $(n - 1)$ o de los menores de orden r, en que $0 < r < n$. Finalmente, el método empleado en el Ejercicio 6 puede ampliarse para demostrar que el signo del término es independiente del método de desarrollo.

Como se señaló anteriormente, los desarrollos (v - 18) y (v - 19) son casos especiales de este teorema siendo $r = 1$. El ejemplo siguiente ilustra el teorema para los casos en que $r = 2$, $n = 4$, y en que se han elegido las dos primeras filas.

Este procedimiento es mucho más útil si varios menores de las filas r de la matriz correspondiente son iguales a cero, como en

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \cdot \begin{vmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{vmatrix} - \begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} \cdot \begin{vmatrix} a_{32} & a_{34} \\ a_{42} & a_{44} \end{vmatrix}$$

$$+ \begin{vmatrix} a_{11} & a_{14} \\ a_{21} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} a_{32} & a_{33} \\ a_{42} & a_{43} \end{vmatrix} + \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \cdot \begin{vmatrix} a_{31} & a_{34} \\ a_{41} & a_{44} \end{vmatrix}$$

$$- \begin{vmatrix} a_{12} & a_{14} \\ a_{22} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} a_{31} & a_{33} \\ a_{41} & a_{43} \end{vmatrix} - \begin{vmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{vmatrix}.$$

(v - 24), donde se ha elegido la primera y segunda filas y $r = 2$ (Ejercicio 9).

(V - 24)
$$\begin{vmatrix} 1 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{vmatrix}.$$

El Teorema v - 10 también es importante porque puede usarse para demostrar el Teorema v - 11 referente a productos de matrices cuadradas. El mismo procedimiento puede usarse para dos matrices cualesquiera tales que el número de columnas de la primera matriz sea igual al número de filas de la segunda matriz. La multiplicación de matrices es sumamente importante en las teorías matemáticas. Consideraremos varias aplicaciones de este procedimiento en el Capítulo v - 15.

Definiremos primero el *producto interno* de dos n-tuplos ordenados tales como

$$V = a_1, a_2, a_3, \ldots, a_n,$$
$$W = b_1, b_2, b_3, \ldots, b_n$$

como la suma de los productos de los elementos correspondientes,

$$a_1b_1 + a_2b_2 + a_3b_3 + \cdots + a_nb_n.$$

En seguida definiremos el *producto de las matrices cuadradas* $M = [a_{ij}]$ y $N = [b_{ij}]$ de orden n como una matriz cuadrada $[c_{ij}]$ de orden n, en donde c_{ij} es el producto interno del conjunto de elementos de la i-ésima fila de M y del conjunto de elementos de la j-ésima columna de N, es decir,

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \cdots + a_{in}b_{nj}.$$

Al estudiar las transformaciones geométricas en el Cap. v - 15 se evidenciará la importancia de esta definición. Esta importancia se debe en parte a la propiedad que se establece en el siguiente teorema:

TEOREMA v - 11. *El determinante del producto de dos matrices es igual al producto de sus determinantes.*

Por ejemplo, puede obtenerse la igualdad siguiente de la definición precedente y del Teorema v - 11:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{vmatrix} = \begin{vmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{vmatrix}.$$

Esta igualdad puede verificarse fácilmente por medio de los polinomios (determinantes) que resultan de los esquemas. También, según el Teorema v - 10, el producto anterior es igual al determinante

$$D = \begin{vmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ -1 & 0 & b_{11} & b_{12} \\ 0 & -1 & b_{21} & b_{22} \end{vmatrix}.$$

Según el Teorema v - 9, cada elemento de la tercera columna de la matriz de D puede reemplazarse por el mismo más b_{11} veces el elemento correspondiente de la primera columna más b_{12} veces el elemento correspondiente de la segunda columna. Análogamente, la cuarta columna puede reemplazarse por ella misma más b_{21} veces la primera columna más b_{22} veces la segunda columna. Luego tenemos una nueva matriz con el mismo determinante D:

$$\begin{vmatrix} a_{11} & a_{12} & a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21} & a_{22} & a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{vmatrix},$$

y según el Teorema v - 10, este determinante es igual a

$$\begin{vmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{vmatrix}.$$

Valiéndonos de los Teoremas v - 9 y v - 10 hemos demostrado el Teorema v - 11 para el caso especial de dos matrices de orden dos.

En general, dadas dos matrices cuadradas de orden n, como $[a_{ij}]$ y $[b_{ij}]$, podemos valernos del Teorema v - 10 para escribir

$$|a_{ij}| \cdot |b_{ij}| = \begin{vmatrix} |a_{ij}| & 0 \\ F & |b_{ij}| \end{vmatrix},$$

en que 0 es el determinante de una matriz cuadrada de orden n cuyos elementos son todos iguales a cero y F es el determinante de una matriz cuadrada de orden n en que los elementos de la diagonal principal son todos iguales a -1 y todos sus otros elementos iguales a cero. Luego, según el Teorema v - 9, la columna de orden $(n + 1)$ de la matriz de este determinante puede reemplazarse por sí misma más b_{11} veces la primera columna más b_{21} veces la segunda columna más ... más b_{n1} veces la n-ésima columna. Análogamente, las columnas de orden $(n + 1)$, $(n + 2)$, ... y $(2n)$ se reemplazan cada una por ellas mismas más múltiplos de las primeras n columnas. La nueva matriz tiene el mismo determinante que anteriormente, conforme al Teorema v - 9, y, como en el caso especial citado anteriormente, ese determinante tiene la forma que el Teorema v - 10 (Ejercicio 21) exige.

La importancia de los Teoremas v - 9, v - 10, y v - 11 se pondrá en evidencia en los ejercicios siguientes y en las secciones que siguen de este capítulo. Hemos señalado los procedimientos que se utilizan en las demostraciones de estos teoremas. Las demostraciones detalladas se dan como ejercicios y pueden consultarse en la mayoría de los textos sobre matrices y determinantes.

El concepto de un menor de una matriz se aplica de la siguiente manera: Dada cualquiera matriz A de m filas y n columnas (v - 1), pueden obtenerse matrices cuadradas de orden $r(r \leqq m, n)$ eligiendo los elementos de r filas cualesquiera y r columnas de la matriz A. Estas matrices se denominan menores de orden r de la matriz A. La *característica* de la matriz A es el mayor entero r tal que A tenga un menor de orden r con determinante no nulo, es decir, existe un menor de orden r de la matriz A con determinante no nulo y todo menor de A de orden $(r + 1)$ tiene un determinante igual a cero. Por ejemplo, cada una de las matrices siguientes tiene característica dos:

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & 2 & 2 \end{bmatrix}.$$

En el Ejercicio 17 se trata un procedimiento sistemático para determinar la característica de cualquiera matriz.

Dejaremos ahora el estudio de la teoría de los determinantes y matrices y consideraremos algunas de sus aplicaciones; encontraremos aquí que el concepto de característica de una matriz es por demás útil. La mayoría de las aplicaciones se tratarán sin entrar a desarrollar temas que corrientemente se estudian en álgebra (college algebra) y en geometría analítica. En el resto de este texto se usarán sistemas de coordenadas ortogonales cartesianas a menos que se especifique expresamente lo contrario.

EJERCICIOS

1. Demostrar que existen $(C^n_{n-r})^2$ menores de orden r de una matriz de orden n.

2. Escribir los menores de orden dos de una matriz de tercer orden.

3. Por medio de (v-18) y dado que según el Teorema v-8 el determinante de (v-2) puede designarse por

$$\begin{vmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{vmatrix}$$

demuéstrese que el complemento algebraico (cofactor) de a_{jj} es igual a su menor.

4. Valiéndose de la Propiedad C y del Ejercicio 3, demostrar que el complemento algebraico de cualquier elemento a_{ij} es $(-1)^{i+j}$ veces su menor.

5. Ampliar los resultados de los Ejercicios 3 y 4 para demostrar que el complemento algebraico de

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

es igual a su menor.

6. Demostrar que el complemento algebraico de cualquier menor de segundo orden

$$\begin{vmatrix} a_{rs} & a_{ru} \\ a_{ts} & a_{tu} \end{vmatrix}$$

es $(-1)^{r+s+t+u}$ veces su menor.

7. Repetir el Ejercicio 10, Cap. v-9, empleando menores de segundo orden con la tercera y cuarta filas de la matriz correspondiente.

8. Repetir el Ejercicio 10, Cap. v-9, empleando menores de segundo orden con la tercera y cuarta columnas.

9. Desarrollar (v-24) mediante menores de segundo orden con las primeras dos filas de su matriz.

10. Se llama *menor principal* el determinante menor que resulta al tachar filas y columnas de igual índice (por ejemplo, primera y tercera filas, primera y tercera columnas). ¿Cuántos menores principales de segundo orden hay en una matriz de orden n?

11. Escribir todos los menores principales de segundo orden de la matriz del determinante del Ejercicio 17, Cap. v-9.

12. Repetir el Ejercicio 17, Cap. v-9, con los menores de tercer orden usando la primera, segunda y tercera filas de la matriz correspondiente.

13. Escribir los 18 pares de menores de segundo orden de la matriz de un determinante general de cuarto orden (v-23).

14. Escribir cinco matrices cuadradas de tres filas y tres columnas con elementos numéricos. Determinar la característica de cada matriz.

15. Escribir una matriz de cuatro filas y cinco columnas y determinar su característica.

16. Demostrar que la característica de una matriz no varía si se efectúan las siguientes *transformaciones elementales:* intercambio de dos líneas paralelas, multiplicación de todos los elementos de una línea por una constante diferente de cero, sumar a los elementos de una línea los múltiplos de los elementos correspondientes de otra línea paralela.

17. Se dice que una matriz $[a_{jk}]$ se encuentra en su *forma normal* cuando $a_{jk} = 0$ para $j \neq k$ y si para algún entero s, $a_{jj} \neq 0$ para $j \leqq s$, $a_{jj} = 0$ para $j > s$. Ilustrar mediante las siguientes matrices cómo puede reemplazarse cualquiera matriz por una matriz en su forma normal por medio de transformaciones elementales:

$$\begin{bmatrix} 1 & 2 & 4 & 6 \\ 2 & 3 & 5 & 7 \\ 11 & 12 & 14 & 16 \\ 5 & 6 & 8 & 10 \end{bmatrix}, \quad \begin{bmatrix} 2 & 3 & 5 & 7 \\ 4 & 2 & 1 & 3 \\ 3 & 6 & 5 & 4 \\ 2 & -2 & 7 & 5 \end{bmatrix}.$$

18. Repetir los Ejercicios 14 y 15, empleando el método del Ejercicio 17.

19. Expresar en una sola matriz los productos siguientes:

(a) $$\begin{bmatrix} a & b & c \\ d & e & f \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & -1 & 1 \end{bmatrix},$$

(b) $$\begin{bmatrix} x & 0 & 0 \\ a & y & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x & 0 & 0 \\ 0 & y & 0 \\ c & d & e \end{bmatrix}.$$

20. Dar una demostración completa del Teorema v-10.
21. Hacer una demostración completa del Teorema v-11.

V - 11 REGLA DE CRAMER. En el Capítulo v - 1 encontramos que el sistema de ecuaciones

$$\begin{aligned} a_1x + b_1y &= c_1, \\ a_2x + b_2y &= c_2 \end{aligned} \tag{V - 25}$$

tiene una solución única si y sólo si el determinante

$$D = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$$

de los coeficientes es diferente de cero. Aún más, si $D \neq 0$, la solución es $x = D_1/D$, y $= D_2/D$, en que D_1 se obtiene reemplazando en D los coeficientes de x por los términos constantes y D_2 se obtiene análogamente reemplazando los coeficientes de y por los términos constantes, es decir,

$$D_1 = \begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix} \quad \text{y} \quad D_2 = \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}.$$

Una ecuación lineal tal como $x + 3y - 5z = 0$, cuyo término constante es cero y cada término de la izquierda es de primer grado, se denomina *ecuación lineal homogénea*. Si una ecuación lineal tiene un término constante diferente de cero, se denomina *ecuación lineal no homogénea*. El método anterior de resolver dos ecuaciones lineales en dos variables puede ampliarse (Teorema v - 12) para incluir sistemas de ecuaciones lineales en n variables. Puede aplicarse a sistemas arbitrarios de ecuaciones lineales homogéneas y a sistemas de ecuaciones lineales no homogéneas (Cap. v - 12).

Demostraremos que para $n = 3$, el sistema

$$\begin{aligned} a_1x + b_1y + c_1z &= d_1, \\ a_2x + b_2y + c_2z &= d_2, \\ a_3x + b_3y + c_3z &= d_3 \end{aligned} \tag{V - 26}$$

tiene una solución única $x = D_1/D$, y $= D_2/D$, $z = D_3/D$ si y sólo si el *determinante de los coeficientes*

$$D = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \neq 0,$$

y en que D_i resulta de D reemplazando los a_i, respectivamente, por los términos constantes d_i; y D_2 y D_3 resultan análogamente al reemplazar los b_i y los c_i por los d_i. Por ejemplo, dado el sistema de ecuaciones

$$\begin{aligned} x + y + 2z &= 5, \\ x - y + z &= 2, \\ 3x + 2y - 5z &= 7, \end{aligned}$$

podemos evaluar el determinante de los coeficientes

$$D = \begin{vmatrix} 1 & 1 & 2 \\ 1 & -1 & 1 \\ 3 & 2 & -5 \end{vmatrix} = 21$$

y dado que $D \neq 0$, podemos expresar la única solución del sistema como sigue:

$$x = \tfrac{1}{21}\begin{vmatrix} 5 & 1 & 2 \\ 2 & -1 & 1 \\ 7 & 2 & -5 \end{vmatrix} = \tfrac{84}{21} = \tfrac{18}{7},$$

$$y = \tfrac{1}{21}\begin{vmatrix} 1 & 5 & 2 \\ 1 & 2 & 1 \\ 3 & 7 & -5 \end{vmatrix} = \tfrac{25}{21},$$

$$z = \tfrac{1}{21}\begin{vmatrix} 1 & 1 & 5 \\ 1 & -1 & 2 \\ 3 & 2 & 7 \end{vmatrix} = \tfrac{13}{21}.$$

En general, para cualquier sistema (v - 26), podemos considerar A_i el cofactor de a_i (Cap. v - 8) en el determinante de los coeficientes, multiplicar ambos miembros de la primera ecuación por A_1, multiplicar ambos miembros de la segunda ecuación por A_2, multiplicar ambos miembros de la tercera ecuación por A_3 y sumar las ecuaciones que resultan para obtener $Dx = D_1$, ya que según (v - 19) y el Ejercicio 18, Capítulo v - 8, tenemos

$$\begin{aligned} a_1A_1 + a_2A_2 + a_3A_3 &= D, \\ b_1A_1 + b_2A_2 + b_3A_3 &= 0, \\ c_1A_1 + c_2A_2 + c_3A_3 &= 0. \end{aligned}$$

y por definición $d_1A_1 + d_2A_2 + d_3A_3 = D_1$. Análogamente, podemos resolver (v - 26) para y, z, empleando los cofactores de sus coeficientes. Finalmente, para cualquier sistema de n ecuaciones lineales en n variables

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ &\cdot \\ &\cdot \\ &\cdot \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n, \end{aligned}$$

podemos multiplicar ambos miembros de la j-ésima ecuación por el cofactor A_{1j} de a_{1j} siendo $j = 1, 2, \ldots, n$, sumar las ecuaciones que resultan y obtener $Dx_1 = D_1$. Análogamente (Ejercicio 7), por medio de los cofactores A_{2j} podemos obtener $Dx_2 = D_2$, y, en general, A_{kj} se usa para obtener $Dx_k = D_k$. Por consiguiente, tenemos

TEOREMA V - 12. REGLA DE CRAMER. *Un sistema de n ecuaciones lineales en n variables*

$$a_{j1}x_1 + a_{j2}x_2 + \cdots + a_{jn}x_n = b_j, \quad (j = 1, 2, \ldots, n)$$

tiene una solución única $x_k = D_k/D$, en que $D \neq 0$ es el determinante de los coeficientes y D_k $(k = 1, 2, \ldots, n)$ resulta de D al reemplazar los coeficientes de x_k por los términos constantes.

También se puede considerar que este teorema proporciona una condición suficiente para que las n ecuaciones lineales en n variables sean *consistentes*, es decir, tengan por lo menos una solución común. Aplicando el concepto de la característica de una matriz (Cap. v - 10), podemos decir que dos ecuaciones lineales en dos variables (v - 25) son consistentes y tienen una solución común única si la matriz de los coeficientes tiene característica dos. Análogamente, tres ecuaciones lineales en tres variables (v - 26) son consistentes y tienen una solución común única si la matriz de los coeficientes tiene característica tres. En general, n ecuaciones lineales en n variables son consistentes y tienen una solución común única si la matriz de los coeficientes tiene característica n.

Si la característica de la matriz de los coeficientes no es igual a n, el sistema puede ser inconsistente, como por ejemplo,

$$x + y = 1,$$
$$x + y = 2,$$

o el sistema puede ser consistente, pero no tener una solución única. Consideradas gráficamente, las dos rectas

$$x + y = 1,$$
$$2x + 2y = 2$$

coinciden, los tres planos (v - 26) pueden tener una línea en común o pueden coincidir. En consecuencia, la condición citada es suficiente para demostrar la consistencia, pero no necesaria. En el Cap. v - 12 se ofrecerá un criterio exacto (Teorema v - 13) de consistencia para cualquier sistema finito de m ecuaciones lineales en n variables.

EJERCICIOS

Resolver los siguientes sistemas de ecuaciones, por medio de la Regla de Cramer.

1. $x - 2y = 3,$
   $2x - y = 5.$

2. $x + 2y - z = 1,$
   $x + y = 5,$
   $3x - y + 2z = 7.$

3. $3x - 4y + 2z = 11,$
   $x + 4y - 5z = 12,$
   $5x + 2y + 3z = 10.$

4. $x + y + z + w = 5,$
   $x - y + 3w = 2,$
   $y - 2z - w = 4,$
   $x - y + z - w = 7.$

5. Demostrar la Regla de Cramer para el sistema (v-25), como se hizo en el Capítulo v-1, multiplicando cada ecuación por el complemento algebraico (en la matriz de los coeficientes) del coeficiente $x_i = x$, sumando las ecuaciones y resolviendo respecto de x_i. Repetir el procedimiento para las demás variables.

6. Repetir el Ejercicio 5 para (v-26).

7. Hacer una demostración general del Teorema v-12 por medio del método del Ejercicio 5.

V-12 SISTEMAS DE ECUACIONES LINEALES. En el Cap. v-11 consideramos sistemas de n ecuaciones lineales en n variables en que el determinante de los coeficientes era diferente de cero. Consideraremos ahora sistemas arbitrarios finitos de ecuaciones lineales. Dado un sistema de m ecuaciones lineales en n variables

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n &= b_3, \\ &\cdot \\ &\cdot \\ &\cdot \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{aligned} \tag{V-27}$$

definiremos la *matriz de los coeficientes* del sistema como:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

y a la *matriz ampliada* del sistema como:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ a_{31} & a_{32} & \cdots & a_{3n} & b_3 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{bmatrix}.$$

En el sistema (v-25) la matriz y la matriz ampliada son

$$\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix},$$

respectivamente.

La característica de una matriz ampliada de un sistema es siempre por lo menos igual a la característica de la matriz de los coeficientes, dado que todo menor de la matriz de los coeficientes es también un menor de la matriz ampliada. En sistemas de n ecuaciones de n variables (Cap. v-11) si la característica de la matriz de los coeficientes es n, entonces la característica de la matriz ampliada

debe ser también n (ya que la matriz ampliada tiene solamente n filas), y por consiguiente, de acuerdo con las condiciones establecidas por el Teorema v - 12, las dos matrices deben tener la misma característica. En general, se tiene

TEOREMA v - 13. TEOREMA FUNDAMENTAL DE LOS SISTEMAS DE ECUACIONES LINEALES. *Una condición necesaria y suficiente para que un sistema de ecuaciones lineales sea consistente es que la matriz de los coeficientes tenga la misma característica que la matriz ampliada.*

El Teorema v - 13 y el siguiente Teorema v - 14, se demuestran en (Bibliografía Nº 9) y en otros textos sobre determinantes y matrices. Los adoptaremos sin demostración y nos dedicaremos principalmente a sus aplicaciones. Dado que un conjunto de ecuaciones lineales en n variables es consistente si y sólo si los hiperplanos correspondientes ($n > 3$), planos ($n = 3$), o líneas ($n = 2$) que representan tienen por lo menos un punto en común, haremos uso frecuentemente de las aplicaciones geométricas de estos teoremas (Ejercicios 6, 7 y 8).

TEOREMA v - 14. *Si en un sistema de ecuaciones lineales en n variables, la matriz de los coeficientes y la matriz ampliada tienen la misma característica r, entonces se pueden atribuir valores arbitrarios dados a $n - r$ variables y las variables restantes quedarán así univocamente determinadas.*

Este teorema establece esencialmente que la solución general de un sistema de ecuaciones lineales en que ambas matrices tienen característica r, contiene $n - r$ parámetros. También puede demostrarse (Ejercicio 12) que la solución general es lineal en estos parámetros. Por lo tanto las $n - r$ variables elegidas como parámetros deben ser tales que la matriz de los coeficientes de las demás variables tenga característica r.

Dado el sistema de ecuaciones

$$\begin{aligned} x + y &= 2, \\ x - y &= 4, \\ 2x + 2y &= 4, \end{aligned}$$

la matriz de los coeficientes y la matriz ampliada tienen característica dos. Luego el sistema tiene una solución única (ya que también $n = 2$), $x = 3$ e $y = 1$. El sistema

$$\begin{aligned} x + y &= 5, \\ x + y &= 2 \end{aligned}$$

tiene la matriz ampliada de característica dos, mientras que la matriz de los coeficientes tiene característica uno. En consecuencia este sistema es inconsistente, es decir, no existe un par de números que satisfagan ambas ecuaciones. Las rectas representadas por este sistema de ecuaciones son paralelas y distintas. Finalmente, las dos matrices del sistema

$$\begin{aligned} x + y &= 1, \\ 2x + 2y &= 2 \end{aligned}$$

tienen característica uno, el sistema es consistente, las dos rectas representadas coinciden, el valor de una de las variables puede elegirse arbitrariamente (Teorema v · 14), y la solución general puede designarse por $x = c$ e $y = 1 - c$ por medio del parámetro c.

Consideremos ahora el ejemplo siguiente en que $n = 3$. El sistema de ecuaciones

$$\begin{aligned} x \quad\quad - z &= 1, \\ x + y \quad\quad &= 2, \\ y + z &= 1 \end{aligned}$$

tiene la matriz de los coeficientes de característica dos y la matriz ampliada de característica dos. Dado que $n = 3$ y $r = 2$, una de las variables (en este caso una cualquiera) puede usarse como parámetro. Si se elige z como parámetro, el sistema resulta

$$\begin{aligned} x &= 1 + z, \\ x + y &= 2, \\ y &= 1 - z. \end{aligned}$$

Ya que la segunda ecuación es la suma de las otras dos, puede descartarse. Las dos ecuaciones restantes junto con $z = z$ designan a las tres variables del sistema dado en función del parámetro z. A cada valor de z corresponden valores únicos de las variables x e y. Todos los puntos de la recta $x - 1 = 1 - y = z$ satisfacen el sistema dado.

Los ejemplos citados ilustran algunas de las aplicaciones de los Teoremas v - 13 y v - 14. Se considerarán más aplicaciones en los ejercicios siguientes y en las tres secciones que quedan de este capítulo.

EJERCICIOS

1. Demostrar que todo sistema de ecuaciones homogéneas lineales es consistente.

2. Demostrar que si un sistema de ecuaciones lineales homogéneas tiene una solución única, entonces esta solución es $x_1 = x_2 = x_3 = \cdots = x_n = 0$.

3. Demostrar que cualquier sistema finito de ecuaciones lineales en n variables tiene una solución única si y sólo si las características de la matriz ampliada y de la matriz de los coeficientes son ambas iguales a n.

4. En (v-27) suponer que por lo menos un $b_j \neq 0$ y demostrar que a) si $m = n$, el determinante no nulo de la matriz de los coeficientes es una solución suficiente; b) si $m = n + 1$, la condición necesaria para obtener una solución es que el determinante de la matriz ampliada sea nulo.

5. Encontrar la característica de la matriz de los coeficientes, la característica de la matriz ampliada, y todas las soluciones (si fuera necesario, por medio de parámetros) de cada uno de los siguientes sistemas de ecuaciones:

(a) $\begin{aligned} 2x + 3y &= 6, \\ x - y &= 5. \end{aligned}$

(b) $\begin{aligned} x + 3y &= 3, \\ 2x + 6y &= 1. \end{aligned}$

(c) $\begin{aligned} 3x + 5y &= 2, \\ 6x + 10y &= 4. \end{aligned}$

(d) $\begin{aligned} x + y &= 3, \\ x - y &= 1, \\ 2x + y &= 5, \\ 2x - y &= 3. \end{aligned}$

(e) $\begin{aligned} x - z &= 1, \\ x + y &= 2, \\ y + z &= 1. \end{aligned}$

(f) $\begin{aligned} x + y + z &= 2, \\ x - y + z &= 1, \\ y &= 1. \end{aligned}$

(g) $\begin{aligned} x + y + z &= 3, \\ x - y + z &= 1, \\ x + z &= 4. \end{aligned}$

(h) $\begin{aligned} x + y + z &= 2, \\ x - y + z &= 1, \\ y &= 5. \end{aligned}$

(i) $\begin{aligned} x &= 1, \\ x + y &= 2, \\ y + z &= 2. \end{aligned}$

6. Considerar los sistemas de rectas representados por los sistemas de ecuaciones del Ejercicio 5, desde a) hasta d) e indicar qué sistemas a) se cortan en un punto único; b) representan rectas coincidentes; c) no tienen ningún punto común.

7. Considerar los sistemas de planos representados por los sistemas de ecuaciones del Ejercicio 5, letras e) hasta i) e indicar qué sistemas a) se cortan en un

punto único; b) se cortan en una sola recta; c) coinciden; d) no tienen ningún punto común.

8. Comparar los resultados de los Ejercicios 6 y 7 con aquellos del Ejercicio 5 y discutir la importancia geométrica del Teorema v-14.

9. Demostrar que si $m = n - 1$, $b_1 = b_2 = \cdots = b_m = 0$, y la matriz de los coeficientes de (v-27) tiene característica $n - 1$, las razones entre las variables son

$$x_1 : x_2 : x_3 : \cdots : x_n = A_1 : -A_2 : A_3 : \cdots : (-1)^{n-1}A_n,$$

donde A_j es el determinante que resulta al tachar la j-ésima columna en la matriz de los coeficientes (ver Bibliografía Nº 16; págs. 41-42).

10. Aplicar los resultados del Ejercicio 9 a los sistemas siguientes de ecuaciones:

(a) $x + y - z = 0$, $x - y + 2z = 0$.

(b) $2x - 3y + z = 0$, $x - 3y + z = 0$.

11. Comparar con el Teorema v-14, los resultados obtenidos en el Ejercicio 10 Dar la solución completa de cada sistema del Ejercicio 10.

12. Demostrar que la solución general del Teorema v-14 es lineal en los $n - r$ parámetros.

V-13 DEPENDENCIA LINEAL. En el Capítulo v-9 se determinó que $c_1b_1 + c_2b_2 + \cdots + c_nb_n$, (en que los b son elementos cualesquiera y los c son constantes no todos iguales a cero), era una combinación lineal de los elementos b. Este concepto se usó (Ejercicio 20, Cap. v-9) para reemplazar cada elemento, como ser a_{ij}, de una línea de la matriz de un determinante por sí mismo más una combinación lineal de los elementos correspondientes de las demás líneas paralelas, por ejemplo,

$$(V\text{-}28) \qquad a_{1j} + c_2a_{2j} + c_3a_{3j} + \cdots + c_na_{nj}, \ (j = 1, 2, \ldots, n),$$

esto es, para todos los elementos a_{1j} de la primera fila. Por ejemplo, dado el determinante

$$\begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & -2 \\ -1 & -6 & 1 \end{vmatrix},$$

podemos reemplazar los elementos a_{1j} de la primera fila de su matriz por $a_{1j} + 2a_{2j} + a_{3j}$ $(j = 1, 2, 3)$ y obtenemos

$$\begin{vmatrix} 6 & 0 & 0 \\ 3 & 2 & -2 \\ -1 & -6 & 1 \end{vmatrix}$$

sin que el determinante varíe (Teorema v-9). Análogamente, si reemplazamos los elementos a_{i1} de la primera columna de la matriz de

$$\begin{vmatrix} 1 & 11 & 6 & 9 \\ 4 & -3 & 0 & -1 \\ -2 & 7 & 3 & 5 \\ 3 & 6 & -3 & 3 \end{vmatrix}$$

por $a_{i1} + 3a_{i2} + 2a_{i3} - 5a_{i4}$, *obtenemos*

$$\begin{vmatrix} 1 & 11 & 6 & 9 \\ 0 & -3 & 0 & -1 \\ 0 & 7 & 3 & 5 \\ 0 & 6 & -3 & 3 \end{vmatrix}.$$

En cada uno de estos ejemplos hemos empleado relaciones análogas a (v-28) no solamente para un solo conjunto de números sino para varios conjuntos de números correspondientes. En el segundo ejemplo usamos esta relación para los cuatro conjuntos de números correspondientes a_{1j}, a_{2j}, a_{3j}, a_{4j}, $(j = 1, 2, 3, 4)$, es decir

$$\begin{aligned} a_{11} + 3a_{12} + 2a_{13} - 5a_{14}, \\ a_{21} + 3a_{22} + 2a_{22} - 5a_{24}, \\ a_{31} + 3a_{32} + 2a_{33} - 5a_{34}, \\ a_{41} + 3a_{42} + 2a_{43} - 5a_{44}. \end{aligned}$$

En consecuencia hemos considerado la misma combinación lineal para cada uno de los cuatro conjuntos de elementos correspondientes.

En seguida, ampliaremos el concepto de combinación lineal a aquél de dependencia lineal. Se dice que los tres conjuntos de cuatro números cada uno:

$$\begin{matrix} x_1, & x_2, & x_3, & x_4, \\ y_1, & y_2, & y_3, & y_4, \\ z_1, & z_2, & z_3, & z_4, \end{matrix} \qquad \text{(V-29)}$$

son dependientes linealmente si existen constantes a, b, c, no todas iguales a cero tales que

$$ax_j + by_j + cz_j = 0, \quad (j = 1, 2, 3, 4)$$

De aquí que los tres conjuntos de números (v - 29) sean dependientes linealmente si y sólo si el sistema de ecuaciones lineales homogéneas

$$\begin{aligned} ax_1 + by_1 + cz_1 &= 0, \\ ax_2 + by_2 + cz_2 &= 0, \\ ax_3 + by_3 + cz_3 &= 0, \\ ax_4 + by_4 + cz_4 &= 0, \end{aligned}$$

(donde x_j, y_j, z_j son dados y en que hay que determinar las constantes a, b, c) tiene una solución donde por lo menos una de las constantes sea diferente de cero. En consecuencia, según el Teorema v - 14 y el Ejercicio 2, Cap. v - 12, los tres conjuntos de números (v - 29) son dependientes linealmente si y sólo si la matriz de los coeficientes

$$\begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \\ x_4 & y_4 & z_4 \end{bmatrix} \quad \text{o} \quad \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \end{bmatrix}$$

tiene característica menor que tres, es decir, todo determinante de tercer orden de la matriz es nulo.

En general, se dice que m conjuntos

$$\text{(V - 30)} \qquad a_{1j}, a_{2j}, \ldots, a_{nj} \qquad (j = 1, 2, \ldots, m)$$

de n elementos son *dependientes linealmente* si y sólo si existen constantes $c_1, c_2, c_3, \ldots, c_m$ no todas nulas tales que

$$\text{(V - 31)} \qquad \begin{aligned} c_1a_{11} + c_2a_{12} + \cdots + c_ma_{1m} &= 0, \\ c_1a_{21} + c_2a_{22} + \cdots + c_ma_{2m} &= 0, \\ &\vdots \\ c_1a_{n1} + c_2a_{n2} + \cdots + c_ma_{nm} &= 0, \end{aligned}$$

es decir,

$$c_1a_{i1} + c_2a_{i2} + \cdots + c_ma_{im} = 0 \quad (i = 1, 2, \ldots, n).$$

Los conjuntos de elementos (v - 30) son *independientes linealmente* si las relaciones (v - 13) implican $c_1 = c_2 = \ldots = c_m = 0$.

El sistema de ecuaciones lineales homogéneas (v - 31) se utilizará en el Teorema v - 15 para expresar las condiciones necesarias y suficientes para que haya dependencia lineal en conjuntos m cualesquiera de elementos (v - 30) por medio de la matriz

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \tag{V - 32}$$

de los coeficientes de los c. Con todo, antes de considerar más detenidamente este caso general, consideremos geométricamente el caso especial (v - 29) suponiendo que los elementos son números reales.

Podemos considerar que tres números reales cualesquiera son coordenadas de un punto en el espacio euclidiano tridimensional. Por definición, los tres conjuntos (v - 29) son dependientes linealmente si y sólo si los cuatro triples de los números correspondiente satisfacen una relación de la forma

$$ax + by + cz = 0,$$

siendo a, b, c constantes no todas nulas, es decir (suponiendo que los números son reales), los triples de los números correspondientes son coplanares con el origen. Existen interpretaciones geométricas análogas y en cierto sentido más elegantes de la dependencia lineal mediante coordenadas homogéneas respecto de espacios vectoriales. Consideraremos solamente la interpretación citada más elemental que se vale de coordenadas no homogéneas con el fin de evitar la tarea de presentar otros conceptos.

Los tres conjuntos de n números reales cada uno,

$$\begin{aligned} &x_1, \quad x_2, \quad \cdots, \quad x_n, \\ &y_1, \quad y_2, \quad \cdots, \quad y_n, \\ &z_1, \quad z_2, \quad \cdots, \quad z_n, \end{aligned}$$

son dependientes linealmente si y sólo si los n triples de los números correspondientes representan puntos coplanares con el origen. Según el Teorema v - 14, el sistema de ecuaciones

$$ax_1 + by_1 + cz_1 = 0,$$
$$ax_2 + by_2 + cz_2 = 0,$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$ax_n + by_n + cz_n = 0$$

tiene una solución única $a = b = c = 0$ si la matriz

$$\text{(V - 33)} \qquad \begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ \cdot & & \\ \cdot & & \\ \cdot & & \\ x_n & y_n & z_n \end{bmatrix} \quad \text{o} \quad \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \\ z_1 & z_2 & \cdots & z_n \end{bmatrix}$$

tiene característica tres. Este sistema de ecuaciones tiene una solución en la que por lo menos una de las constantes *a, b,* c es diferente de cero si la matriz (v - 33) tiene característica menor que tres. En consecuencia, los tres conjuntos anteriores de n números son linealmente dependientes si y sólo si todo determinante de tercer orden de la matriz (v - 33) es nulo. Si la matriz tiene característica dos, los triples de los números correspondientes representan puntos coplanarios con el origen. Las mismas condiciones en relación a la dependencia lineal rigen aún cuando la interpretación geométrica pueda no ser válida al tratarse de elementos pertenecientes a cualquier anillo.

La discusión anterior referente a tres conjuntos de n elementos cada uno puede ahora ampliarse respecto de m conjuntos de n elementos cada uno (v - 30). Si los elementos son números reales, cada uno de los n conjuntos de los m números reales correspondientes puede tomarse como un punto en el espacio euclidiano m-dimensional. Estos n puntos se encuentran es un hiperplano.

$$c_1a_1 + c_2a_2 + \cdots + c_ma_m = 0$$

que pasa por el origen si y sólo si los conjuntos de elementos (v - 30) son dependientes linealmente. Estas condiciones pueden expresarse como un sistema de ecuaciones (v - 31) que se satisfacen, ya sea que los elementos sean números reales o no. Si $m = n$, los m conjuntos de n elementos cada uno (v - 30) son dependientes

linealmente si y sólo si la matriz (v - 32) tiene característica menor que m, es decir, si y sólo si el determinante de m filas de (v - 32) es nulo. Si $m < n$, entonces, dado que el sistema (v - 31) consiste en n ecuaciones en m incógnitas, los m conjuntos de elementos (v - 30) son dependientes linealmente si y sólo si cada determinante de m filas de (v - 32) es nulo (Teorema v - 14). Si $m > n$ hay menos ecuaciones que las constantes que hay que determinar y los conjuntos son siempre dependientes (Ejercicio 5). Esta situación es análoga a la de encontrar un plano $ax + by + cz = 0$ sobre uno o dos puntos dados como, por ejemplo, cuando los conjuntos dados son

$$x_1, \quad x_2,$$
$$y_1, \quad y_2,$$
$$z_1, \quad z_2.$$

Estos resultados pueden resumirse como sigue:

TEOREMA v - 15. *Si $m > n$, entonces m conjuntos cualesquiera de n elementos cada uno son dependientes linealmente. Si $m \leqq n$, entonces m conjuntos* (v - 30) *de n elementos cada uno son linealmente dependientes si y sólo si todo determinante de m filas de la matriz* (v - 32) *es igual a cero.*

La definición de que los elementos de un conjunto de constantes $b_1, b_2, \ldots, b_n$ son dependientes linealmente si existe una combinación lineal.

$$c_1b_1 + c_2b_2 + \cdots + c_nb_n = 0$$

donde no todos los c son nulos puede hacerse extensiva a conjuntos arbitrarios de elementos. Por ejemplo, siempre que las variables toman valores de un conjunto infinito de números (Cap. III - 1 y Cap. III - 4), m polinomios $f_1, f_2, \ldots, f_m$ en cualquier número de variables son dependientes linealmente si y sólo si existen m constantes c_i no todas nulas tales que

$$c_1f_1 + c_2f_2 + \cdots + c_mf_m = 0$$

para todos los valores de las variables. Esta definición es equivalente (Ejercicio 10) a definir a los polinomios del conjunto como de-

pendientes linealmente si y sólo si los conjuntos de los coeficientes correspondientes son dependientes linealmente. Esta otra forma de la definición puede emplearse en el Teorema v - 15. En el conjunto siguiente de ejercicios consideraremos varios teoremas basados sobre la definición de dependencia lineal y algunas de las numerosas aplicaciones de este concepto.

EJERCICIOS

1. Demostrar que si un conjunto de elementos es una combinación lineal de otros m —1 conjuntos de elementos, entonces los m conjuntos de elementos son dependientes linealmente.

2. Demostrar que si m conjuntos de elementos son dependientes linealmente, entonces por lo menos un conjunto es una combinación lineal de los otros.

3. Demostrar que si existe entre m conjuntos de elementos, k conjuntos que son linealmente dependientes, siendo $k \leq m$, entonces los m conjuntos son dependientes linealmente.

4. Demostrar que si alguno de los m conjuntos de elementos está compuesto exclusivamente de ceros, entonces los m conjuntos son linealmente dependientes.

5. Demostrar que si $m > n$, m conjuntos cualesquiera de n elementos cada uno son dependientes linealmente. (Indicación: ampliar el sistema a m conjuntos de m elementos cada uno agregando ceros).

6. Indicar cuáles de los conjuntos siguientes, de cuatro números cada uno, son dependientes linealmente:

(a) 3, 0, 1, 5,
1, −2, −1, 2,
2, 2, 2, 3.

(b) 2, 2, 1, 3,
3, 5, 2, 4,
1, −1, 0, 2.

(c) 1, 0, 1, 1,
0, 1, 1, 0,
1, 1, 0, 0

(d) 1, 2, 3, 4,
2, 4, 6, 8,
a, b, c, d.

7. Demostrar que los tres polinomios

$$a_j x + b_j y + c_j z + d_j \qquad (j = 1, 2, 3)$$

son dependientes linealmente si y sólo si los tres conjuntos de números

$$a_j, b_j, c_j, d_j \qquad (j = 1, 2, 3)$$

son dependientes linealmente.

8. Señalar cuáles de los conjuntos siguientes de polinomios son dependientes linealmente:

(a) $3x + y + 2$, $y - 1$, $x + y + 2$.
(b) $x + 1$, $y + 1$, $x + y$.
(c) $x + 2y + 3z + 4$, $2x + 4y + 6z + 8$, $ax + by + cz + d$.
(d) $x + 2y - z + 5$, $8z - 12y - 10$, $3x + z + 10$.

9. Demostrar que los gráficos de las ecuaciones correspondientes a cualquier conjunto finito de polinomios dependientes linealmente de la forma $a_1x + b_1y + c_1z$, tienen todos por lo menos un punto de intersección común.

10. Demostrar que la dependencia lineal de cualquier conjunto finito de polinomios en cualquier número finito de variables que adquieren valores de un conjunto infinito de números, implica la dependencia lineal de los conjuntos de constantes de sus conjuntos de coeficientes, y a la inversa.

V-14 APLICACIONES EN GEOMETRIA ANALITICA. Algunos textos elementales de geometría analítica consideran la aplicación de determinantes y matrices a la geometría.

En todos los textos superiores de geometría donde se emplean métodos analíticos, el estudio de los determinantes y las matrices constituye una parte muy importante (Cap. v - 15). En esta sección ampliaremos los conceptos de geometría usados en el estudio de la dependencia lineal (Cap. v - 13), solamente enumerando algunas de las aplicaciones corrientes de los determinantes y matrices en la geometría analítica elemental. En seguida, en la sección siguiente, concluiremos nuestro estudio de los determinantes y de las matrices con una breve revisión de sus aplicaciones a las transformaciones geométricas.

El área de un triángulo con vértices en (x_1, y_1), (x_2, y_2), (x_3, y_3) está dada por

$$\pm \left(\tfrac{1}{2}\right) \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix},$$

en que debe elegirse el signo de modo que el área no sea negativa. Este resultado puede ampliarse para dar

$$\begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = 0$$

como una condición necesaria y suficiente para que los tres puntos sean colineales. También puede usarse en la forma

$$\begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x & y & 1 \end{vmatrix} = 0$$

para encontrar la ecuación de la recta determinada por dos puntos dados distintos (x_1, y_1) y (x_2, y_2).

En un plano, dos rectas

$$a_1x + b_1y = c_1,$$
$$a_2x + b_2y = c_2$$

tienen un punto en común único si las matrices

$$\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{bmatrix}$$

tienen ambas características dos; y las rectas coinciden si las dos matrices tienen característica uno y son paralelas si las matrices tienen características diferentes (Teorema v - 13 y v - 14). Análogamente, en el espacio tri-dimensional dos planos

$$a_1x + b_1y + c_1z = d_1,$$
$$a_2x + b_2y + c_2z = d_2$$

tienen una recta única en común si en este sistema de ecuaciones la matriz de los coeficientes y la matriz ampliada tienen ambas característica dos; estos dos planos coinciden si ambas matrices tienen característica uno y son paralelos si las matrices tienen diferentes características. Los conceptos del Cap. v - 12 pueden también usarse para demostrar que tres planos

$$a_jx + b_jy + c_jz = d_j \qquad (j = 1, 2, 3)$$

tienen un punto único en común si las matrices correspondientes tienen ambas característica tres; los tres planos tienen una recta única en común si ambas matrices tienen característica dos y coinciden si las dos matrices tienen características uno; no tienen ningún punto en común si las matrices son de características diferentes. En el Ejercicio 7 se consideran más correspondientes entre los planos y las características de las matrices.

El volumen de un tetraedro cuyos vértices son (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3), (x_4, y_4, z_4) está dado por

$$\pm \left(\frac{1}{6}\right) \begin{vmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{vmatrix},$$

en donde, como anteriormente, hay que elegir el signo de modo que el volumen no resulte negativo. También, como anteriormente, se puede ampliar este resultado para dar

$$\begin{vmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{vmatrix} = 0$$

como una condición necesaria y suficiente para que los cuatro puntos dados sean coplanarios. Tres puntos en el espacio (x_j, y_j, z_j), $j = 1, 2, 3$, son no-colineales si y sólo si

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} \neq 0,$$

y la ecuación del plano determinado por tres puntos dados no colineales está dada por

$$\begin{vmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x & y & z & 1 \end{vmatrix} = 0.$$

Hasta aquí hemos visto que la ecuación de una recta determinada por dos puntos distintos cualesquiera y la ecuación del plano determinado por tres puntos no-colineales pueden expresarse por medio de determinantes. También el área de un triángulo y el volumen de un tetraedro pueden expresarse por medio de las coordenadas de sus vértices y de determinantes. Ejemplos como éstos ilustran la aplicación de los determinantes y de las matrices en geometría analítica. En los ejercicios siguientes se examinarán unos cuantos ejemplos más; en (Bibliografía Nº 16) pueden consultarse muchos ejemplos.

EJERCICIOS

1. Determinar cuáles de los siguientes triples de puntos sobre un plano son colineales. Si no son colineales, encontrar el área del triángulo que determinan:

a) (1,2), (5,6), (17,18).
b) (—1,5), (1,4), (3,0).
c) (11,7), (6,2), (—1,3).

2. Por medio de determinantes indicar las ecuaciones de las rectas determinadas por los siguientes pares de puntos:

a) (1,2), (5,6).
b) (—1,5), (1,4).
c) (11,7), (6,2).
d) (912, —13), (—115,76).

3. Determinar cuáles de los siguientes conjuntos de puntos en el espacio son coplanarios. Si no son coplanarios, encontrar el volumen del tetraedro que ellos determinan:

a) (1, 2, 3), (4, 5, 6), (7, 8, 9), (10, 11, 12).
b) (2, —2, 0), (5, 7, 11) (—7, 3, 12), (1, 1, 1).
c) (1, —1, 1), (7, 13, 27), (5, 2, 1), (—6, 3, 4).

4. Valiéndose de determinantes, indicar en los Ejercicios que se señalan la ecuación del plano que pasa por los cuatro puntos o las ecuaciones de las caras (planos) del tetraedro a) Ejercicio 3 a); b) Ejercicio 3 b); c) Ejercicio 3 c).

5. Describir en el plano los gráficos de los conjuntos de ecuaciones del Ejercicio 5 desde a) hasta d), Cap. v-12.

6. Describir en el espacio los gráficos de los conjuntos de ecuaciones del Ejercicio 5 desde e) hasta i), Cap. v-12.

7. Determinar las características de la matriz de los coeficientes y de la matriz ampliada de un sistema de ecuaciones que representa

a) tres planos que tienen un punto común único;
b) tres planos distintos que tienen una recta común;
c) tres planos que tienen un plano en común;
d) tres planos paralelos;
e) dos planos paralelos y un tercer plano que los corta;
f) dos planos coincidentes y un tercer plano que los corta;
g) dos planos coincidentes y un tercer plano paralelo a ellos;
h) tres planos distintos tales que los pares de planos se corten en tres rectas paralelas.

8. Demostrar (Bibliografía Nº 16; pág. 87), que la recta determinada por dos planos que se cortan

$$a_1x + b_1y + c_1z + d_1 = 0,$$
$$a_2x + b_2y + c_2z + d_2 = 0$$

tiene números de dirección

$$\begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix}, \quad \begin{vmatrix} c_1 & a_1 \\ c_2 & a_2 \end{vmatrix}, \quad \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}.$$

(*Indicación:* Valerse del Ejercicio 9, Cap. v-12. Los números de dirección se definen en los textos de geometría analítica que incluyen geometría de los sólidos).

9. Aplicar el resultado del Ejercicio 8 a las rectas determinadas por

(a) $x + y - z + 2 = 0,\ x - y + 2z - 5 = 0,$
(b) $2x + 3y - z - 3 = 0,\ x - 5y + z + 2 = 0.$

V - 15. TRANSFORMACIONES GEOMETRICAS. La definición de Félix Klein señala la importancia de las transformaciones en geometría: Una geometría cualquiera es un estudio de las propiedades (expresadas por definiciones y teoremas) que permanecen invariantes respecto de un grupo de transformaciones. Por ejemplo, en la geometría euclidiana estudiamos propiedades tales como la longitud, el área, la magnitud de los ángulos, líneas paralelas, triángulos semejantes y congruentes que permanecen invariantes sometidas a movimientos rígidos, es decir, traslaciones y rotaciones. Cada una de estas transformaciones puede expresarse como una matriz con referencia a un sistema de coordenadas.

Dado el plano xy corriente que se emplea en geometría analítica, podemos representar cualquiera traslación en el plano por el sistema de ecuaciones:

(V-34) $$x' = x + a, \quad y' = y + b.$$

Por ejemplo, usando los ejes en las posiciones convencionales, si todos los puntos se mueven dos unidades a la derecha, tenemos:

$$x' = x + 2, \quad y' = y;$$

si todos los puntos se mueven tres unidades hacia abajo, tenemos:

$$x' = x, \quad y' = y - 3;$$

si todos los puntos se mueven dos unidades a la derecha y tres unidades hacia abajo, tenemos:

$$x' = x + 2, \quad y' = y - 3.$$

En general, dado que cualquiera traslación en el plano puede considerarse como el resultado de un movimiento a lo largo del eje de las x y un movimiento a lo largo del eje y, tenemos (v-34) para cualquiera traslación en el plano. Análogamente, se demuestra en geometría analítica que cualquiera rotación alrededor del origen en el plano puede expresarse en la forma:

(V-35) $$x' = x \cos \theta - y \operatorname{sen} \theta, \quad y' = x \operatorname{sen} \theta + y \cos \theta.$$

También se puede demostrar que si a la rotación (v - 35) le sigue una traslación (v-34), tenemos una transformación de la forma:

$$x' = x \cos \theta - y \operatorname{sen} \theta = a, \quad y' = x \operatorname{sen} \theta + y \cos \theta + b.$$

Ahora trataremos métodos de denotar estas transformaciones por medio de matrices.

Cada una de las transformaciones anteriores se representa por ecuaciones de la forma:

$$x' = a_{11}x + a_{12}y + a_{13}, \quad y' = a_{21}x + a_{22}y + a_{23}.$$

Además, cada transformación está completamente determinada por los a_{jk}, es decir, por una matriz de la forma:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}.$$

Ampliando esta matriz usaremos una matriz de tercer orden de la forma:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{bmatrix},$$

que resulta de sumar la tercera fila de la matriz identidad (Ejercicio 6), de modo que las matrices de las dos transformaciones puedan multiplicarse (Cap. v-10) y que la matriz del producto tenga la misma forma que las matrices dadas. Encontraremos que un producto ordenado de las matrices de dos transformaciones es

la matriz de una transformación que resulta al aplicar las dos transformaciones dadas, una después de la otra en cierto orden. Muchos de los ejercicios que figuran al final de esta sección se refieren a esta propiedad.

Ya hemos visto que cualquiera traslación (v-34) y cualquiera rotación alrededor del origen (v-35) pueden representarse respectivamente por las matrices

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Análogamente, cualquier punto (x, y) del plano puede representarse por una matriz. Lo mismo que en el caso anterior, se elige la forma de la matriz de modo que permita la multiplicación de ciertas matrices. Usaremos una matriz con una columna y tres filas:

$$\begin{bmatrix} x \\ y \\ 1 \end{bmatrix}.$$

Esta convención nos permitirá expresar las ecuaciones de una transformación como una sola igualdad por medio de matrices.

Se dice que dos matrices son *iguales* si y sólo si tienen el mismo número de filas, el mismo número de columnas y si sus elementos correspondientes son idénticos. Dos matrices relacionadas mediante transformaciones elementales (Ejercicio 16, Cap. v-10) tienen la misma característica, pero no son necesariamente iguales en el sentido que se ha expresado aquí. La igualdad de dos matrices de mn elementos es equivalente, según la definición anterior, a un sistema de mn ecuaciones. Luego, al multiplicar matrices, podemos expresar la traslación (v-34) por medio de la ecuación

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x + a \\ y + b \\ 1 \end{bmatrix}.$$

Dado que la primera y la última matriz son iguales si y sólo si los elementos correspondientes son iguales, la igualdad citada de las matrices es precisamente equivalente a (v-34). Análogamente, (v-35) es equivalente a

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta & 0 \\ \operatorname{sen}\theta & \cos\theta & 0 \\ 0 & 0 & \end{bmatrix} \cdot \begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix}.$$

La relación entre la expresión de una traslación o rotación mediante un sistema de ecuaciones lineales entre las coordenadas y en términos de una matriz (en cierto sentido la matriz de los coeficientes del sistema de ecuaciones) puede comprenderse rápidamente (Ejercicios 1 y 2), de modo que será tan fácil obtener una representación como la otra. Una ventaja de la representación por medio de matrices se desprende de la facilidad con que se obtiene el resultado de una sucesión de transformaciones como producto (tomado en el orden inverso) de las matrices correspondientes. La traslación que resulta como una sucesión de dos traslaciones y que hemos citado anteriormente en la explicación de una traslación puede expresarse como:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix}.$$

En el caso especial de dos traslaciones no tiene importancia el orden en que se multipliquen las matrices (Ejercicio 5), pero, en general, encontraremos que debe considerarse el orden.

La transformación que resulta de considerar dos transformaciones en orden se denomina *producto ordenado* de esas dos transformaciones. Análogamente, podemos considerar el producto ordenado de cualquier número finito de transformaciones. La importancia del orden se debe a que si a la traslación (v-34) le sigue la rotación (v-35) se obtiene

$$\text{(V-36)} \qquad \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta & a\cos\theta - b\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta & a\operatorname{sen}\theta + b\cos\theta \\ 0 & 0 & 1 \end{bmatrix},$$

mientras que si se hace primero la rotación y, en seguida, la traslación, se tiene

$$\text{(V-37)} \qquad \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta & a \\ \operatorname{sen}\theta & \cos\theta & b \\ 0 & 0 & 1 \end{bmatrix}.$$

Estos resultados pueden verificarse fácilmente multiplicando las matrices de las transformaciones en el orden opuesto a aquél en que se usan las transformaciones (Ejercicio 3).

El hecho de que (v-36) y (v-37) son, en general, diferentes, denota que el efecto de una traslación seguida de una rotación es diferente de aquél de una rotación seguida de la traslación. Por ejemplo, sea la traslación $x' = x + 2$, $y' = y$, y la rotación $x' = -x$, $y' = -y$. El punto (3,6) queda en (5,6) al hacer la traslación (suponiendo que el sistema de coordenada permanece fijo); el punto (5,6) queda en (—5,—6) al hacer la rotación, es decir, la traslación seguida de la rotación lleva al punto (3,6) a la posición (—5,—6). Análogamente, el punto (3,6) se lleva al punto (—3,—6) por la rotación y el punto (—3,—6) queda en (—1—6) por la traslación, es decir, la rotación seguida de la traslación lleva el punto (3,6) a (—1,—6). Por consiguiente, hemos encontrado que la aplicación de transformaciones y la multiplicación de matrices no son operaciones conmutativas (Ejercicio 4).

Las transformaciones (v-34) a (v-37) de la geometría euclidiana pueden considerarse como casos especiales de las transformaciones en geometrías más generales. Cualquiera transformación (transformación afín) del plano euclidiano en sí mismo (Bibliografía Nº 52, págs. 117-118), puede representarse por una matriz de la forma

$$\text{(V-38)} \qquad \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ 0 & 0 & 1 \end{bmatrix},$$

en que $a_1b_2 - a_2b_1 \neq 0$. Si $b_1 = a_2 = 0$ y $a_1 = b_2 = 1$, entonces (v-38) representa una traslación; si $c_1 = c_2 = 0$, $a_1 = b_2$, $a_2 = -b_1$ y $a^2_1 + a^2_2 = 1$, entonces (v - 38) representa una rotación. Cualquier movimiento rígido en el plano (transformación euclídiana) puede expresarse como el producto de una traslación y una rotación (posiblemente en el espacio) y puede representarse por una matriz de la forma

$$\text{(V - 39)} \qquad \begin{bmatrix} a & b & c_1 \\ -be & ae & c_2 \\ 0 & 0 & 1 \end{bmatrix},$$

donde $a^2 + b^2 = 1$ y $e^2 = 1$ (Ejercicios 13, 14). Si $e = 1$ (v-39)

es equivalente a (v-37) (Ejercicio 15); si $e = -1$, debe incluirse una rotación en el espacio o una línea de reflexión en el plano.

Dado que cualquiera geometría puede considerarse como un estudio de las propiedades invariantes (Ejercicio 9) con respecto a grupos de transformaciones y que estas transformaciones pueden representarse por matrices, esta sección podría ampliarse hasta constituir un libro completo. Nos hemos limitado a indicar cómo dos transformaciones corrientes pueden expresarse por medio de matrices (v-34) y (v-35) y a señalar que estas transformaciones son simplemente casos especiales de transformaciones más generales, tales como (v-38) en geometría, de las que la geometría euclidiana es un caso especial. En (Bibliografía Nº 35), se podrá consultar un estudio completo de las razones por las cuales la geometría euclidiana es un caso especial de varias otras geometrías.

En este capítulo hemos definido los determinantes de matrices cuadradas de cualquier orden n por medio de permutaciones y hemos examinado el empleo de los determinantes y de las matrices en el estudio de sistemas de ecuaciones lineales, dependencia lineal, geometría analítica y transformaciones geométricas. Nuestro examen estuvo, por necesidad, restringido a un pequeño número de aplicaciones típicas. Estudios más completos de la teoría y sus aplicaciones pueden consultarse en los textos señalados en la Bibliografía, Nºs 9, 16, 39, 44 y 49.

EJERCICIOS

1. Representar las siguientes traslaciones por medio de matrices:

(a) $x' = x - 1,\ y' = y + 2.$
(b) $x' = x + 2,\ y' = y + 5.$
(c) $x' = x - 3,\ y' = y - 4.$

2. Representar las siguientes rotaciones en torno al origen por medio de matrices: a) 30°, b) 45°, c) 120°, d) 180°, e) 270°.

3. Deducir las matrices (v-36) y (v-37) de (v-34) y (v-35).

4. Ilustrar el hecho de que la multiplicación de las matrices no es conmutativa valiéndose de las matrices

$$\begin{bmatrix} a & b & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} d & e & f \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

5. Demostrar, valiéndose de dos matrices generales de la forma (v-34), que el producto de dos traslaciones cualesquiera es a) una traslación; b) conmutativa.

6. Demostrar que

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

representa la transformación identidad en el plano, es decir, si se multiplica por cualquiera otra matriz de tres filas y tres columnas, o si es multiplicada por ella, el producto es igual a la otra matriz.

7. Escribir en una sola transformación, valiéndose de matrices, los productos de las transformaciones que se señalan en los siguientes ejercicios: a) Ejercicio 1 (a) y 2 (a); b) Ejercicios 1 (a) y 1 (b); c) Ejercicios 1 (b) y 2 (c); d) Ejercicios 1 (c) y 2 (d); e) Ejercicios 1 (c) y 2 (e); f) Ejercicios 2 (a) y 2 (d).

8. Demostrar, valiéndose del resultado del Ejercicio 6, que la traslación $x' = x - a, y' = y - b$ es la inversa de (v-34).

9. Un conjunto de transformaciones afines (v-38) forma un grupo si el conjunto contiene el inverso de todas las transformaciones del conjunto y el producto de todos los pares de transformaciones del conjunto. Demostrar que esta definición está de acuerdo con la definición general de grupo dada en el Capítulo I-14.

10. Demostrar que el conjunto de todas las traslaciones (v-34) forma un grupo.

11. Demostrar que el conjunto de todas las rotaciones en torno al origen forma un grupo.

12. Demostrar que el conjunto de todas las transformaciones afines (v-38) forma un grupo.

13. Demostrar que (v-34) y (v-35) tienen cada cual la forma (v-39), cuando $a^2 + b^2 = e^2 = 1$.

14. Demostrar que (v-36) y (v-37) tienen cada cual la forma (v-39) cuando $a^2 + b^2 = e^2 = 1$.

15. Demostrar que (v-39) puede escribirse en la forma (v-37) cuando $a^2 + b^2 = e^2 = 1$.

16. Demostrar que una traslación queda determinada por un par de puntos correspondientes.

17. Cualquiera *reflexión de un punto* puede expresarse en la forma

$$x' = -x + a, \qquad y' = -y + b.$$

Indicar la representación correspondiente a una reflexión de un punto por medio de una matriz. ¿Forma un grupo el conjunto de todas las reflexiones de un punto? Explicar.

18. Demostrar que el producto de un número par de reflexiones de un punto es una traslación.

19. Demostrar que el producto de un número impar de reflexiones de un punto es una reflexión de un punto.

20. Demostrar que el conjunto de todas las reflexiones de un punto y de todas las traslaciones forma un grupo.

21. Cualquiera *dilatación* puede expresarse en la forma

$$x' = ax + b, \qquad y' = ay + c, \qquad \text{en que } a \neq 0, 1.$$

Indicar la representación correspondiente de una dilatación por medio de una matriz. ¿Forma un grupo el conjunto de todas las dilataciones? Explicar.

22. El conjunto de todas las dilataciones y traslaciones constituye el conjunto de las *transformaciones homotéticas*. Demostrar que el conjunto de todas las transformaciones homotéticas forma un grupo.

23. Demostrar que el conjunto de todas las matrices con determinantes no nulos forma un grupo si las matrices tienen la forma

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

24. Demostrar que el conjunto de todas las matrices de la forma

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

con determinantes no nulos forma un grupo.

CAPITULO VI

Construcciones

Las construcciones geométricas interesan a jóvenes y adultos. A los niños les gusta hacer decoraciones para la mesa de sus fiestas de cumpleaños, de Navidad o de otras ocasiones especiales. Probablemente, el gusto por hacer canastos de papel, pegarles el asa, pintarles los lados, está estimulado por la ilusión de tener el canasto lleno de dulces en la fiesta. A medida que el niño crece la afición por las construcciones geométricas puede manifestarse en juegos con reglas, compases y transportadores, haciendo estrellas, tarjetas de saludo y, más tarde, construyendo cuerpos geométricos. Algunos adultos pasan del papel y la goma de pegar al tallado en madera y a los trabajos en metal. Otros, construyen modelos de trenes, barcos y aun ciudades completas. Unos pocos deciden desafiar a las autoridades matemáticas y tratan de resolver el problema clásico de trisectar un ángulo (Cap. VI, Secciones 6 a 8). El irresistible atractivo de las construcciones geométricas puede brindar muchas horas felices a jóvenes y adultos.

En este capítulo nos referiremos a construcciones en la geometría plana euclidiana. Aprenderemos (Cap. VI-4) que las construcciones clásicas que emplean solamente regla y compás pueden usarse para efectuar las cuatro operaciones racionales y la extracción de raíz cuadrada. Es así como —dada una recta cualquiera con un origen y un punto unidad para designar la unidad de distancia y el sentido positivo o dirección sobre la recta—, podemos asociar a los enteros positivos con puntos que resultan de agregar unidades sobre la recta; y los enteros negativos con puntos que resultan al

sustraer unidades; y los números racionales con puntos que resultan por multiplicación y división. En otras palabras, podemos construir sobre una recta el conjunto de puntos racionales respecto de un origen dado y del punto unidad. En general, dados el origen y el punto unidad, podemos construir todos los puntos sobre la recta, cuyas coordenadas se puedan expresar por medio de un número finito de números racionales, de operaciones racionales y de extracción de raíces cuadradas. Aún más, estos son los únicos puntos sobre la recta que pueden construirse a partir de los puntos dados empleando únicamente regla y compás (Cap. VI-3). En consecuencia, existen criterios algebraicos precisos para determinar si un punto dado sobre una recta puede construirse o no a partir del origen dado y con la unidad de longitud dada, mediante los métodos clásicos. Análogamente, existen criterios algebraicos para determinar si es posible o no construir una figura plana. Estos criterios algebraicos son la base de las consideraciones que haremos aquí sobre las construcciones geométricas en este estudio de los conceptos fundamentales del álgebra. Analizaremos las construcciones clásicas en el plano desde un punto de vista algebraico (Cap. VI, Secciones 3 y 4), aplicaremos nuestros conceptos algebraicos para demostrar la imposibilidad de tres famosos problemas clásicos de construcción (Cap. VI-6) y consideraremos varias construcciones no clásicas (Cap. VI, Secciones 7 y 8) de uno de estos problemas: la trisección de ángulos arbitrarios.

Este estudio de las construcciones geométricas desde un punto de vista algebraico permite vislumbrar las relaciones esenciales entre el álgebra (considerada como un estudio de conjuntos de números y variables y de sus relaciones entre sí) y la geometría (considerada como un estudio de conjuntos de puntos, rectas, planos, etc. y sus relaciones entre sí). En los fundamentos de las matemáticas hay teorías básicas y conceptos que se aplican indistintamente al álgebra o a la geometría. Nosotros no nos hemos empeñado en alcanzar este esencia común a todas las matemáticas. No obstante, esperamos que el estudio, en este capítulo, de las operaciones racionales, desde los puntos de vista algebraico y geométrico, y de la representación geométrica de ciertas funciones algebraicas corrientes —en el próximo capítulo—, contribuirán, en cierto modo, a que el lector aprecie la interdependencia entre el álgebra y la geometría.

VI-1 CONSTRUCCIONES CLASICAS.

Las construcciones geométricas pueden clasificarse en dos conjuntos, según sean los métodos e instrumentos que se empleen. Los griegos de la antigüedad se empeñaron en hacer todas las construcciones geométricas elementales usando solamente compás y regla. La regla puede usarse únicamente para trazar rectas. No está permitido utilizar el largo o el ancho de la regla, ni hacer marcas sobre ella. Nos referiremos a las construcciones que se atengan a estas restricciones con el nombre de *construcciones clásicas*. Las construcciones que se hacen con reglas graduadas, transportadores, mecanismos articulados, etc. (Cap. VI-9) se denominarán *construcciones no clásicas*.

Teóricamente, las construcciones hechas con regla y compás son absolútamente precisas. Sin embargo, en la práctica, no son ni más ni menos exactas que las construcciones con transportador y regla graduada. Muchos de los problemas que se consideran difíciles o imposibles sujetos a las restricciones clásicas son sencillos si se usan marcas sobre la regla, transportador, reglas paralelas, pantógrafo, trisector de ángulos, mecanismos articulados y otros recursos análogos. Birkhoff y Beatley consideran construcciones con regla graduada y transportador (Bibliografía Nº 6, págs. 165-171), así como también construcciones con regla y compás solamente (Bibliografía Nº 6, págs. 172-196). Fourrey (Bibliografía Nº 20), considera varios tipos de construcciones incluyendo construcciones sólo con regla, construcciones únicamente con compás y construcciones con regla y compás.

Para las construcciones, tanto clásicas como no clásicas, vamos a suponer que todos los puntos, rectas, etc., se encuentran en el mismo plano euclidiano. Para las construcciones clásicas daremos por aceptadas las cinco suposiciones siguientes:

(i) Por dos puntos dados cualesquiera se puede trazar una línea recta.

(ii) Se puede trazar un círculo que tenga por centro cualquier punto dado y por radio cualquier segmento de recta dado.

(iii) Es posible determinar la intersección de dos rectas dadas no paralelas cualesquiera.

(iv) Es posible determinar las intersecciones de cualquiera recta dada y de cualquiera circunferencia dada, en caso de que éstas existan.

(v) Es posible determinar las intersecciones de dos circunferencias dadas, siempre que éstas existan.

Toda construcción clásica debe consistir en un número finito de pasos por medio de regla y compás. Dado que las cinco suposiciones anteriores incluyen todos los pasos posibles con regla y compás, toda construcción clásica debe consistir en un número finito de pasos, en donde cada paso depende de una de las suposiciones anteriores.

EJERCICIOS

1. Formular suposiciones algebraicas equivalentes a cada una de las cinco suposiciones fundamentales de las construcciones clásicas.

2. Hacer las siguientes construcciones empleando únicamente una regla (Bibliografía Nº 20; págs. 3-24):

a) Dado un segmento de recta AB y una recta m paralela a AB, encontrar el punto medio del segmento AB.

b) Dadas dos rectas paralelas y un punto P, construir una recta paralela a las rectas dadas que pase por P.

c) Dadas las rectas $x = 0$, $x = 1$, $y = 0$, $y = 1$ de un sistema de coordenadas en un plano, construir o describir las construcciones de los puntos $(2,0)$, $(3,0)$, $(k,0)$, $(0, 2)$, $(0, 3)$, $(0, n)$, (k, n) en que k y n son enteros cualesquiera.

3. Hacer las siguientes construcciones usando únicamente compás (Bibliografía Nº 20; págs. 95-114):

a) Dados tres puntos en el plano, determinar si son o no colineales.

b) Dada una recta m y un segmento AB sobre ella, construir un segmento AF sobre m de una longitud igual a cinco veces la de AB.

c) Dados dos puntos cualesquiera A y B, construir, sin considerar la recta AB, un punto C colineal con AB de tal modo que la longitud de AC sea dos veces aquella de AB.

d) Dados los puntos $(0, 0)$, $(0, 1)$, $(1, 0)$, ilustrar y describir una construcción para cualquier punto entero (k, n) como en el Ejercicio 2(c).

4. En el siglo XVIII, Mascheroni descubrió que cualquier punto que pudiera construirse empleando regla y compás, podía también construirse utilizando únicamente compás. Demostrar que las cinco construcciones fundamentales, que se dan por aceptadas en las construcciones clásicas, excepto la primera, pueden efectuarse empleando únicamente compás (Bibliografía Nº 13; págs. 140-152).

VI-2 CONSTRUCCIONES CLASICAS ELEMENTALES. Desde los tiempos de la antigüedad griega, los geómetras se han sentido atraídos por el gran número

de construcciones que pueden hacerse utilizando únicamente regla y compás, es decir, por las construcciones clásicas. Actualmente, la mayoría de los textos de geometría para la enseñanza media incluyen algunas construcciones clásicas elementales. En particular, el Nº 6 de la Bibliografía; págs. 172-196, contiene una muestra excelente de construcciones clásicas, que incluye a aquéllas que se presentan como ejercicios al final de esta sección. Estos ejercicios servirán, principalmente, como un repaso de las construcciones corrientes que se estudian en la escuela secundaria. En unos pocos casos se dan indicaciones. Algunas de estas construcciones pueden simplificarse mucho por medio de teoremas más avanzados de la geometría euclidiana. También resulta un buen ejercicio suplementario hacer las demostraciones geométricas o algebraicas de cada construcción. Aunque la lista de ejercicios es larga y pudo haber sido mucho más larga, hay también muchas construcciones que no son posibles empleando únicamente regla y compás. En las tres secciones siguientes estudiaremos los fundamentos algebraicos para determinar si es posible o no hacer una construcción determinada valiéndose únicamente de regla y compás.

EJERCICIOS

Hacer las construcciones siguientes utilizando únicamente regla y compás:

1. La simetral de un segmento de recta dado.
2. Un ángulo igual a un ángulo dado.
3. La bisectriz de un ángulo dado.
4. Una recta que pase por un punto dado y sea paralela a una recta dada.
5. Dividir un segmento de recta dado en n partes iguales.
6. Dividir un segmento de recta dado en partes proporcionales a k segmentos de recta dados.
7. La cuarta proporcional de tres segmentos de recta dados, es decir, construir n si $r/s = m/n$.
8. La perpendicular a una recta dada en un punto dado que se encuentre a) sobre la recta, y b) fuera de ella.
9. La media proporcional (medio geométrico) entre dos segmentos de recta dados; es decir, construir s si $m/s = s/n$.
10. La circunferencia que pase por tres puntos dados no colineales.
11. La circunferencia circunscrita a un triángulo dado.
12. La circunferencia inscrita en un triángulo dado.
13. El centro de una circunferencia, dado un arco de ella.

14. La tangente a una circunferencia dada en un punto dado.

15. Las tangentes a una circunferencia dada desde un punto fuera de ella.

16. Las tangentes exteriores comunes a dos circunferencias dadas, en el caso en que sea posible. (*Indicación:* Dadas dos circunferencias de centros *O*, *O'* y de radios r y r' respectivamente, en que $r \geq r'$, construir una circunferencia con centro de radio $r - r'$ y valerse del Ejercicio 15, tomando *O'* como punto exterior).

17. Las tangentes interiores comunes a dos circunferencias dadas, en el caso de que existan. (*Indicación:* Esta construcción puede hacerse de manera análoga a la empleada en el Ejercicio 16, construyendo primero una circunferencia de radio $r + r'$ en torno de *O*).

18. Un triángulo que tenga tres lados dados.

19. Un triángulo que tenga dos lados y el ángulo comprendido dados.

20. Un triángulo que tenga dos ángulos y un lado dados. (*Indicación:* Dados dos ángulos cualesquiera de un triángulo, el tercer ángulo puede encontrarse valiéndose del hecho de que en la geometría euclidiana, la suma de tres ángulos de un triángulo es un ángulo extendido).

21. Un triángulo (no es siempre único) que tenga dados dos lados y el ángulo opuesto a uno de ellos.

22. Trisectar un ángulo recto.

23. Inscribir polígonos regulares de tres, seis y doce lados en una circunferencia dada.

24. Inscribir polígonos regulares de cuatro, ocho y dieciseis lados en una circunferencia dada.

25. Inscribir polígonos de cinco y diez lados en una circunferencia dada.

26. Inscribir un polígono regular de quince lados en una circunferencia dada. [*Indicación:* valerse de un lado o del ángulo del centro de un exágono (seis lados) regular inscrito y lo mismo de un decágono (diez lados) regular inscrito].

27. Circunscribir a una circunferencia dada polígonos regulares de tres, cuatro, cinco, seis, ocho, diez y doce lados.

VI-3 EL PUNTO DE VISTA ALGEBRAICO. Los geómetras griegos idearon muchas construcciones con regla y compás. Sin embargo, trataron en vano de resolver mediante construcciones clásicas problemas tales como la duplicación de un cubo, la cuadratura de un círculo, y la trisección de un ángulo (Cap. VI-6). Durante el siglo diecinueve se dieron demostraciones algebraicas para probar que estos tres problemas no pueden resolverse exclusivamente con regla y compás (Cap. VI-6). Sin embargo, pueden resolverse, mediante construcciones no clásicas. En general, el criterio algebraico o analítico sobre las posibilidades de construcción (Cap. VI-4 y Cap. VI-5) per-

mite determinar exactamente qué problemas de construcción clásicos tienen solución, es decir, qué problemas de construcción se pueden resolver valiéndose únicamente de regla y compás. Por ejemplo, las consideraciones algebraicas llevaron a la construcción clásica de un polígono regular de 17 lados cuya posibilidad de construcción de acuerdo con las restricciones clásicas, ni siquiera se sospechó durante los veinte siglos transcurridos desde los tiempos de Euclides hasta la época de Gauss (Bibliografía Nº 15, pag. 353).

Las proposiciones algebraicas correspondientes a las cinco suposiciones formuladas en el Cap. VI-1, son:

(i') Se puede determinar la ecuación de una recta que pasa por dos puntos dados.

(ii') Es posible establecer la ecuación de una circunferencia que tenga un centro y un radio dados.

(iii') Es posible determinar las coordenadas del punto de intersección de dos rectas dadas cualesquiera no paralelas.

(iv') Es posible determinar las coordenadas de los puntos de intersección de una recta dada y de una circunferencia dada, en el caso de que estos puntos existan.

(v') Es posible determinar las coordenadas de los puntos de intersección de dos circunferencias dadas, en caso de que éstos existan.

Todos los resultados anteriores pueden hallarse algebraicamente empleando coordenadas cartesianas ortogonales, las cuatro operaciones racionales y la extracción de raíces cuadradas reales; e inversamente, sólo pueden resolverse por medio de regla y compás problemas que sean algebraicamente equivalentes a los citados anteriormente. Por lo tanto, existe un criterio algebraico para determinar si alguna construcción particular puede o no realizarse empleando únicamente regla y compás. Estos criterios se formulan más fácilmente mediante las cuatro operaciones racionales y la extracción de raíces cuadradas. En la sección siguiente consideraremos construcciones clásicas bien determinadas, las *construcciones clásicas básicas* que pueden utilizarse para efectuar estas cinco operaciones.

VI-4 CONSTRUCCIONES CLASICAS BASICAS. Acabamos de señalar que toda construcción clásica posible debe ser equivalente algebraicamente a un número finito de pasos en que se usen sólo las cuatro operaciones racio-

nales y la extracción de raíces cuadradas. Ahora vamos a verificar que estas cinco operaciones pueden realizarse utilizando únicamente regla y compás.

Dados los segmentos de recta de longitud m y n, respectivamente, podemos construir fácilmente segmentos de longitud m, n, $m + n$, y $m - n$ sobre cualquiera recta dada. Si se da además un segmento de longitud igual a la unidad, podemos construir segmentos de longitud mn y m/n como en la Fig. VI-1. Estas dos cons-

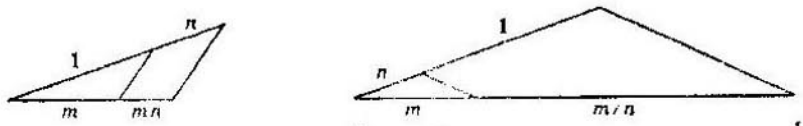


FIG. VI-1

trucciones se basan en que una recta paralela a un lado de un triángulo divide a los otros dos lados en la misma razón. Por consiguiente, tenemos las proporciones $mn : m = n : 1$ y $m : (m/n) = n : 1$, respectivamente, en los triángulos de la Fig. VI-1. Después de esto, podemos sumar, sustraer, multiplicar y dividir segmentos de recta en el sentido que hemos señalado, utilizando únicamente regla y compás, es decir, se pueden efectuar las cuatro operaciones racionales por medio de construcciones clásicas.

La extracción de raíz cuadrada es un caso especial de hallar el medio geométrico o la media proporcional (Ejercicio 9, Cap. VI-2). La demostración de esta construcción clásica se basa en que cualquier triángulo inscrito en una semicircunferencia es un triángulo rectángulo. Así el $\triangle ABC$ en la Fig. VI-2 es un triángulo rectángulo. El segmento CD es perpendicular a AB en D, siendo $AD = m$ y $DB = n$. Luego, los triángulos ADC y CDB son semejantes y $AD/CD = CD/DB$, de donde $CD = \sqrt{mn}$. El caso especial $\sqrt{m}$ en que estamos empeñados, pueden efectuarse haciendo $n = 1$) para cualquier segmento de recta dado de longitud m mediante los métodos clásicos si se da un segmento de longitud igual a la unidad (o bien, se puede obtener de los datos dados mediante los métodos clásicos).

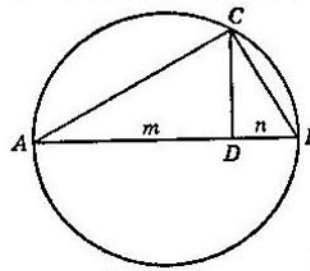


FIG. VI-2

Dado un segmento de longitud igual a la unidad y segmentos m y n, podemos construir segmentos $m + n$, $m - n$, $m \cdot n$, m/n y $\sqrt{mn}$, es decir, hemos verificado ahora que, dado un segmento de longitud igual a la unidad, pueden combinarse segmentos de recta dados cualesquiera por medio de las cuatro operaciones racionales y de la extracción de raíz cuadrada empleando únicamente regla y compás. A la inversa, dado que toda construcción clásica debe constar de un número finito de aplicaciones de las cinco suposiciones fundamentales (Cap. VI-1) y cada una de ellas debe efectuarse por medio de las cuatro operaciones racionales y la extracción de raíces cuadradas, hemos demostrado que toda construcción clásica debe constar de un conjunto finito de construcciones clásicas básicas. Ahora bien, definiremos una *figura geométrica plana* como cualquier conjunto de puntos y rectas en un plano, y obtenemos el

TEOREMA VI-1. *Es posible construir una figura geométrica plana por medio de regla y compás si y sólo si las coordenadas cartesianas ortogonales de sus puntos (vértices, etc.) pueden obtenerse de aquéllas de la figura dada, mediante un número finito de operaciones racionales y extracciones de raíces cuadradas reales.*

Todos los números racionales y expresiones, tales como $\sqrt{10 - 2\sqrt{5}}$ pueden construirse con regla y compás una vez que se haya elegido una unidad. La expresión citada es la longitud de un lado de un pentágono regular inscrito en un círculo de radio dos. En la sección que sigue veremos que toda expresión susceptible de construirse como aquélla es una raíz de una ecuación irreducible con coeficientes enteros de grado igual a una potencia entera de 2.

EJERCICIOS

1. Dado un segmento como unidad, construir segmentos de longitudes iguales a 3, $\frac{3}{4}$, 2, $2 + \sqrt{5}$, $\sqrt{3 + \sqrt{2}}$.
2. Dividir un segmento de recta dado en cinco partes iguales
3. Dividir un segmento de recta dado en partes proporcionales a tres segmentos de recta dados.
4. Construir una estrella de cinco puntas.

5. Construir un exágono regular, dado su lado.

6. Dado un triángulo obtusángulo, construir las circunferencias inscrita y circunscrita.

7. Hacer una demostración algebraica de la construcción de un decágono regular (Bibliografía Nº 13; págs. 122-123), (Bibliografía Nº 6; págs. 191-194).

8. Dado el eje x, el origen y el punto (1,1) en un plano, construir los puntos: a) (4,0); b) $(-\frac{3}{2}, 0)$; c) $(-5 + \sqrt{2}, 0)$; d) (2,3); e) $(\sqrt{3}, \sqrt{5})$.

9. Id. al Ejercicio 8, construir los gráficos de a) $x = 5$; b) $2x + 3y = 6$; c) $\sqrt{3}x + 4y = 2\sqrt{3}$.

10. Demostrar que el gráfico de cualquier recta con coeficientes constructibles puede ser construída por los métodos clásicos.

11. Demostrar que cualquiera circunferencia

$$x^2 + y^2 + bx + dy + e = 0$$

cuyos coeficientes pueden construirse, puede también construirse.

VI-5 CONSTRUCCIONES DE RAICES DE ECUACIONES. Toda ecuación lineal tiene una raíz que puede expresarse por medio de los coeficientes, empleando únicamente operaciones racionales. En consecuencia, cualquiera ecuación lineal con coeficientes susceptibles de construirse tiene una raíz que es posible construir y que se representa por un número. Se dice que este número es constructible si es posible obtener el segmento de recta correspondiente de los datos dados, cualesquiera sean las restricciones que se hayan establecido. En esta sección nos dedicaremos a números cuya construcción es posible únicamente con regla y compás.

Cualquiera ecuación cuadrática puede escribirse en la forma

$$x^2 - ax + b = 0 \qquad \text{(VI-1)}$$

Las raíces de esta ecuación son precisamente (Bibliografía Nº 15; págs. 355-356) las intersecciones con el eje x, de la circunferencia

$$\left(x - \frac{a}{2}\right)^2 + \left(y - \frac{b+1}{2}\right)^2 = \frac{a^2 + (b-1)^2}{4}, \qquad \text{(VI-2)}$$

que queda reducida a

$$\left(x - \frac{a}{2}\right)^2 = \frac{a^2}{4} - b$$

cuando $y = 0$. Cualquiera ecuación cuadrática con coeficientes susceptibles de construirse puede expresarse en la forma (VI-1), donde a y b son constructibles. Las coordenadas del centro y el

radio de la circunferencia (VI-2) son, por lo tanto, susceptibles de construir. En consecuencia, las raíces reales de cualquiera ecuación cuadrática con coeficientes susceptibles de construir pueden construirse siempre que tales raíces reales existan. Ya hemos demostrado

TEOREMA VI - 2. *Si los coeficientes de una ecuación lineal o cuadrática pueden construirse basándose sobre los datos dados empleando únicamente regla y compás, entonces las raíces reales de la ecuación pueden construirse empleando únicamente regla y compás.*

Consideraremos en seguida unos cuantos resultados de ecuaciones de grado mayor que dos. Sin embargo, no intentaremos exponer una teoría completa sobre estas ecuaciones.

En el anillo de los polinomios con coeficientes enteros (Cap. III - 2) un polinomio dado $p(x)$ es reducible dentro del anillo de los enteros (Cap. III - 6) si y sólo si puede expresarse en la forma $p(x) = q(x) \cdot r(x)$, en donde $q(x)$ y $r(x)$ son polinomios de grado positivo con coeficientes enteros. En particular, cualquier polinomio no lineal con coeficientes enteros y una raíz racional es reducible dentro del anillo de los enteros. Si una ecuación irreducible $f(x) = 0$ con coeficientes racionales tiene una raíz susceptible de construirse r, esto significa que tiene una raíz que puede expresarse por medio de las operaciones racionales y la extracción de raíces cuadradas. Luego (según teorías más avanzadas de álgebra) todas las raíces de $f(x) = 0$ son conjugadas de r y pueden obtenerse de r exactamente como $1 - \sqrt{2}$ puede obtenerse de $1 + \sqrt{2}$. Por ejemplo, el número $\sqrt{10 - 2\sqrt{5}}$ que se mencionó al final del Cap. VI - 4 es una raíz de $x^4 - 20x^2 + 80 = 0$. Esta ecuación tiene las raíces $\sqrt{10 - 2\sqrt{5}}$, $\sqrt{10 + 2\sqrt{5}}$, $-\sqrt{10 - 2\sqrt{5}}$, $-\sqrt{10 + 2\sqrt{5}}$. En general, el grado de cualquiera ecuación irreducible que tenga una raíz real susceptible de construir debe ser de la forma $d = 2^k$, en donde k es un entero no negativo. Esto resulta evidente intuitivamente, ya que cualquiera raíz racional es una raíz de una ecuación irreductible de grado $1 = 2^0$ y cualquiera raíz irracional susceptible de construirse es una de entre un número par de raíces conjugadas (incluyendo ella misma) que resulta de la raíz dada al considerar cada uno de los radicales alternadamente como positivos y negati-

vos. Sea $f(x) = 0$ una ecuación polinomia con coeficientes racionales que tenga precisamente como raíces las 2^m conjugadas obtenidas de esta manera. Luego $f(x)$ tiene grado 2^m. Sin embargo, con este método de calcular las raíces conjugadas puede ocurrir que algunas raíces se cuenten más de una vez, como por ejemplo, cuando el número dado cuya construcción es posible, es

$$\sqrt{5 - \sqrt{2} + \sqrt{3}} + \sqrt{5 + \sqrt{2} - \sqrt{3}}.$$

En estos casos puede demostrarse (Bibliografía Nº 30; págs. 5-12) que toda raíz se cuenta exactamente s veces, para algún s entero positivo, siendo s divisor de m, y que si $g(x) = 0$ es una ecuación polinomia irreducible con coeficientes racionales que tiene como raíz el número dado que es susceptible de construir, entonces $g(x) = 0$ tiene como raíces las raíces distintas de $f(x) = 0$ y $f(x) = c[g(x)]^s$, siendo c una constante. Por lo tanto, el grado d de $g(x)$ satisface la relación $d^s = 2^m$, de donde $d = 2^k$ para algún entero positivo k. Como consecuencia de este resultado tenemos

TEOREMA VI - 3. *Una ecuación polinomia irreductible con coeficientes racionales y de grado d, en que d no pueda expresarse como una potencia entera de 2, no tiene ninguna raíz que pueda construirse valiéndose únicamente de regla y compás con la unidad de longitud dada.*

Nótese que no se pueden construir todas las raíces reales de las ecuaciones polinomias irreducibles con coeficientes racionales y de grado 2^m para todo entero m (Cap. IV - 5). Al estudiar algunos de los problemas clásicos de construcción en el Cap. VI - 6, nos servirá mucho el Teorema VI - 3.

EJERCICIOS

1. Hacer una lista de cinco números irracionales constructibles.

2. Elegir un segmento de recta como unidad y construir los números de la lista hecha en el Ejercicio 1.

3. Indicar el conjunto de conjugados asociados con cada uno de los números dados en el Ejercicio 1.

4. Indicar una ecuación irreductible con coeficientes enteros para cada número del Ejercicio 1 y que tenga el número dado como raíz.

5. Dado un sistema de coordenadas, construir las raíces de las siguientes ecuaciones:

a) $3x - 5 = 0$;

b $x^2 - 6x - 1 = 0$;

c) $2x^2 + 5x - 3 = 0$;

d) $x^3 + 3x^2 - 1 = 0$.

6. Encontrar los conjugados distintos de cada uno de los siguientes números:

$$1 + \sqrt{2}, \quad 2 - \sqrt{3 + \sqrt{2}}, \quad \sqrt{1 + \sqrt{2 - \sqrt{1 - \sqrt{2}}}}.$$

7. Hallar una ecuación irreducible con coeficientes enteros que se satisfaga con cada uno de los números dados en el Ejercicio 6.

8. Dar ejemplos de tres ecuaciones polinomias con coeficientes enteros que no puedan resolverse gráficamente utilizando únicamente regla y compás.

9. Se puede demostrar (Bibliografía Nº 15; pág. 379) que un polígono regular de n lados puede construirse usando únicamente regla y compás, si y sólo si

$$n = 2^k p_1 p_2 \cdots p_m,$$

en que los p_j son números primos distintos de la forma $2^{2^j} + 1$. Indicar en la fórmula anterior todos los valores de $n \leqq 30$ tales que un polígono regular de n lados pueda construirse mediante regla y compás. (Gauss fue el primero en descubrir una fórmula para este resultado cuando él era aún muy joven y este hecho influyó grandemente en su decisión de consagrar su vida a las matemáticas).

VI-6 PROBLEMAS DE CONSTRUCCION FAMOSOS. Hay tres problemas clásicos de construcción que han constituido un desafío para los geómetras durante muchos siglos: la construcción de un cubo cuyo volumen sea el doble de aquél de un cubo dado (la "duplicación" de un cubo), la construcción de un cuadrado cuya área sea igual a aquélla de un círculo dado (la "cuadratura" de un círculo), y la trisección de cualquier ángulo dado. Estos problemas fueron conocidos por los griegos de la antigüedad y aún hoy día se proponen soluciones de ellos. No obstante, en la actualidad podemos valernos de criterios algebraicos (Cap. VI - 3 y Cap. VI - 5) para establecer que es imposible resolver estos problemas conforme a las restricciones clásicas. En las Secciones 7 y 8 de este Capítulo VI examinaremos unos cuantos métodos no clásicos para resolver el problema de la trisec-

ción y haremos notar la manera en que cada solución contraviene las restricciones clásicas.

Construcción de un cubo cuyo volumen sea el doble de aquél de un cubo dado. Este problema es llamado a veces *problema de Delos.* De acuerdo con la tradición, este problema surgió cuando el oráculo de Delos aconsejó a los atenienses que duplicaran la medida del altar de Apolo. Si se elige como unidad de longitud la arista del cubo dado, se necesita construir un segmento de recta de longitud x tal que $x^3 = 2$. La ecuación $x^3 - 2 = 0$ es irreducible en el anillo de los polinomios con coeficientes enteros, ya que según el Teorema IV - 9 no tiene una raíz racional, luego, según el Teorema VI - 3, no tiene una raíz susceptible de construirse. En consecuencia, no es posible construir $x = \sqrt[3]{2}$ y el problema de Delos no puede resolverse empleando únicamente regla y compás. El problema puede resolverse fácilmente por métodos no clásicos. Por ejemplo, podemos hacer el gráfico de la curva $y = x^3$ y hallar su intersección con la recta $y = 2$.

Construcción de un cuadrado cuya área sea igual a aquélla de un círculo dado. Si elegimos como unidad de longitud el radio de un círculo dado, el problema se reduce a la construcción de una raíz de la ecuación $x^2 = \pi$, lo que sólo es posible si el número trascendente (Cap. I - 10) π es susceptible de construirse. A continuación observamos que según las limitaciones clásicas todo número susceptible de construirse es algebraico (Cap. I - 10) y por lo tanto, ningún número trascendente puede construirse valiéndose únicamente de regla y compás. Dado que de acuerdo a las restricciones clásicas todo número susceptible de construirse puede expresarse por medio de números enteros empleando las operaciones racionales y la extracción de raíces cuadradas, todo número cuya construcción es posible satisface una ecuación polinomia con coeficientes enteros y en consecuencia es un número algebraico. Es así como el número trascendente $\sqrt{\pi}$ no es constructible por medio de los métodos clásicos, y la construcción de un cuadrado cuya área sea igual a aquélla de un círculo dado no puede realizarse empleando únicamente regla y compás.

En 1882, Lindemann demostró, por primera vez, que π es un número trascendente. No obstante, las construcciones no clásicas de π se conocen desde hace muchos siglos (Bibliografía Nº 30; págs. 55-80). Hacia el año 400 a. J. C. Hipias de Elis hizo una

construcción no clásica de una curva conocida con el nombre de cuadratriz (Bibliografía Nº 55; págs. 19-20), que podía usarse para obtener π y para trisectar cualquier ángulo. Brevemente, dado un cuadrante de un círculo OAB, como en la Fig. VI - 3, se considera un punto Q que se mueve con velocidad constante a lo largo del arco AB y un punto R que se mueve con velocidad constante a lo largo del radio OB de tal modo que los dos puntos parten simultáneamente de A y O, respectivamente, y llegan simultáneamente a B. En cualquier instante t_1 podemos designar las posiciones de los puntos por R_1 y Q_1. El lugar geométrico BPD de la intersección de radio OQ_1 y de la recta correspondiente paralela a OA que pasa por R_1 constituye la *cuadratriz*. La cuadratriz puede obtenerse también deslizando el punto R a lo largo de la recta OB a una velocidad constante y haciendo girar el círculo en torno de O a una velocidad constante.

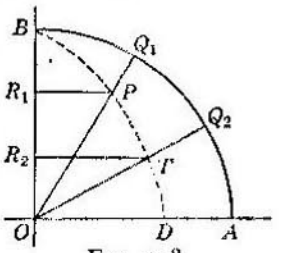


FIG. VI-3

La ecuación de la cuadratriz puede obtenerse de las relaciones

$$y = ct, \qquad \text{arc tg } y/x = kt, \tag{VI - 3}$$

en que $P:(x, y)$ es un punto general de la cuadratriz y t indica el tiempo en que las partículas Q y R han estado en movimiento. Elijamos la unidad de tiempo de modo que a medida que R se mueva desde O hasta B, t varíe de 0 a 1. Luego $\pi/2 = k$, e $y/x = \text{tg } \pi t/2$ es una ecuación de la cuadratriz. Si elegimos también la unidad de longitud de modo que $OB = 1$, tenemos que $1 = c$, de donde $y = t$ y $x = t/\text{tg } (\pi t/2)$. Si $t = 0$, esta relación puede usarse para obtener $OD = 2/\pi$ por medio de los métodos que se estudian en cálculo para tratar fórmulas indeterminadas. En consecuencia, $2/\pi$ y por lo tanto, π puede construirse por medio de la cuadratriz, regla y compás.

La trisección de un ángulo dado. Este problema es aún muy popular por cuanto todavía se proponen soluciones casi todos los años. Estas soluciones son inevitablemente construcciones no clásicas, aunque a menudo no sea esa la intención. Consideraremos primeramente una demostración algebraica de la imposibilidad del problema de la trisección conforme a las restricciones clásicas

y en seguida (Cap. VI - 7 y Cap. VI - 8) consideraremos unas cuantas soluciones no clásicas.

La demostración corriente para probar que existe por lo menos un ángulo que no puede trisectarse por medio de los métodos clásicos se vale de unas pocas identidades trigonométricas y de un ángulo de 120°. Dado un ángulo de 120° buscamos un ángulo de 40°. La construcción de un ángulo de 40° es equivalente a la construcción de un triángulo rectángulo cuya hipotenusa es la unidad y su base es cos 40°. De esta manera un ángulo de 120° puede trisectarse si y sólo si se puede construir un segmento de recta de longitud cos 40°. De cos 120° $= -\frac{1}{2}$ y de la identidad trigonométrica

$$4\cos^3 x - 3\cos x = \cos 3x,$$

podemos obtener la relación

$$4\cos^3 40^\circ - 3\cos 40^\circ + \tfrac{1}{2} = 0.$$

Haciendo $y = \cos 40^\circ$, tenemos

$$4y^3 - 3y + \tfrac{1}{2} = 0.$$

Multiplicando por 2 y haciendo la sustitución $z = 2y$, resulta

$$z^3 - 3z + 1 = 0$$

esta ecuación no tiene raíces racionales (Teorema IV - 9) y por consiguiente es irreducible en el anillo de los polinomios con coeficientes enteros. Luego, según el Teorema VI - 3, su raíz no puede construirse y $z = 2\cos 40^\circ$ no es constructible, es decir, un ángulo de 120° no puede trisectarse y el problema de la trisección no es posible conforme a las restricciones clásicas.

La demostración anterior mediante los Teoremas IV - 9 y VI - 3, de que ninguna raíz z es susceptible de construirse puede expresarse también de una manera más sencilla, como sigue: Las únicas raíces racionales posible de la ecuación $z^3 - 3z + 1 = 0$ deben ser enteros, dado que el coeficiente principal es la unidad y cualquiera raíz racional debe ser divisor del término constante. Por lo tanto, las únicas raíces racionales posibles son $+1$ y -1. Dado que ninguno de estos enteros es una raíz, la ecuación no tiene raíces racionales. Si la ecuación tuviera una raíz expresable por medio de irracionales cuadráticos tal como $a + b\sqrt{2}$, tendría

también como raíz al irracional conjugado $a - b\sqrt{2}$ y la raíz restante (la tercera) sería racional. Dado que cualquier número cuya construcción es posible mediante los métodos clásicos puede expresarse por medio de enteros utilizando un número finito de operaciones racionales y la extracción de raíces cuadradas, todo número no racional susceptible de construirse forma parte de un conjunto de un número par de conjugados (incluso él mismo) (Cap. VI - 5). Por lo tanto, cualquiera ecuación con coeficientes enteros que tenga una raíz irracional susceptible de construirse, debe tener un número par de raíces irracionales. En particular, cualquiera ecuación cúbica con coeficientes enteros que tenga por lo menos una raíz irracional susceptible de construirse debe tener exactamente dos raíces irracionales y una raíz racional. En consecuencia, si la ecuación cúbica citada no tiene ninguna raíz racional, esto implica que no tiene ninguna raíz susceptible de construirse. Como en el caso anterior, esto implica que un ángulo de 120° no puede trisectarse, de donde se deduce que no todo ángulo puede trisectarse y que el problema de la trisección no puede resolverse usando únicamente regla y compás. En las dos secciones que siguen consideraremos unos cuantos métodos no clásicos para trisectar ángulos y veremos en qué contravienen las restricciones clásicas.

EJERCICIOS

1. ¿Es posible dividir un ángulo arbitrario en siete partes iguales conforme a las restricciones clásicas? Explicar.

2. Indicar una construcción clásica de dieciseis puntos cualesquiera de la elipse

$$x^2/4 + y^2 = 1.$$

3. ¿Se puede hacer el gráfico completo de la elipse del Ejercicio 2 conforme a los métodos clásicos? Explicar.

4. Proponer una construcción no clásica de la elipse del Ejercicio 2.

5. Formular las condiciones necesarias y suficientes que deben cumplir los coeficientes de la ecuación $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ para que pueda dibujarse el gráfico completo de la ecuación utilizando únicamente regla y compás (Cap. VII-3).

VI-7 TRISECCIONES GEOMETRICAS NO CLASICAS. En una de las más antiguas y más sencillas construcciones de la trisección de ángulos se desestima la limi-

tación clásica de que no debe usarse marcas en la regla. Esta construcción se atribuye a Arquímedes. Necesita solamente compás y una regla con dos marcas en ella. Una regla graduada servirá muy bien.

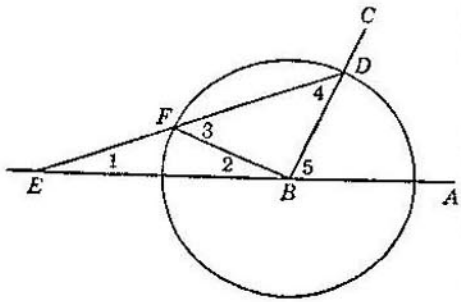


Fig. VI-4

Dado cualquier ángulo agudo ABC (Fig. VI-4) constrúyase una circunferencia de radio r en torno al vértice B. Sea D la intersección de la circunferencia con el lado BC. Prolónguese el lado AB más allá de B. Márquese en la regla la longitud $r = BD$. En seguida manténgase la regla sobre D y deslícese una marca a lo largo de la prolongación de AB hasta que la otra marca toque a la circunferencia en algún punto F. Trácese DF y prolónguese hasta que corte a AB en E. Entonces $\angle BEF = \frac{1}{3} \angle ABC$. Esto se demuestra como sigue: Trácese BF y designese los ángulos como en la Fig. VI-4. Entonces $EF = FB = BD = r$, $\angle 1 = \angle 2$, $\angle 3 = \angle 4$. Dado, que $\angle 3$ es un ángulo exterior del triángulo BEF y $\angle 5$ es un ángulo exterior del triángulo BED, tenemos $\angle 3 = \angle 1 + \angle 2 = \angle 1 + \angle 1$; $\angle 5 = \angle 1 + \angle 4 = \angle 1 + \angle 3 = \angle 1 + \angle 1 + \angle 1$, y por consiguiente $\angle ABC = \angle 3\ BEF$. Esta no es una solución clásica del problema de la trisección, ya que se emplean marcas sobre la regla.

Hipias de Elis hacia el año 400 A. C. (Cap. VI-6) ideó otra solución no clásica del problema de la trisección. Este método se vale de la cuadratriz (Fig. VI-3). De las relaciones (VI-3), tenemos

$$\angle AOQ_2 : \angle AOQ_1 = OR_2 : OR_1$$

de donde el ángulo AOQ_1 puede trisectarse haciendo $OR_2 = \frac{1}{3} OR_1$, R_2T paralela a OA, y trazando OTQ_3. Entonces $\angle AOQ_2 = \frac{1}{3} \angle AOQ_1$. Esta solución del problema de la trisección no satisface las restricciones clásicas dado que la cuadratriz no puede dibujarse exactamente mediante los métodos clásicos.

Varias soluciones que se han propuesto para el problema de la trisección constan de una sucesión de pasos en que se trazan rectas

tan cerca como se desee de las rectas pedidas que trisectarían al ángulo. Estas soluciones no satisfacen las restricciones clásicas, dado que se deben trazar las rectas pedidas en un número finito de pasos.

La popularidad del problema de la trisección se manifiesta en el número siempre creciente de inventores de métodos para trisectar ángulos. El *Chicago Sun* del 5 de enero de 1948, publicaba un artículo titulado "¿Trisectar un ángulo? Sencillo... El insiste". La construcción descrita en el artículo se vale de un círculo de diámetro igual al ancho de la regla empleada, coloca el ángulo superior izquierdo de la regla a lo largo de cierta recta, y manipula la regla hasta que el ángulo superior derecho toque a otra recta. Aunque esta construcción no utiliza marcas sobre la regla, se vale del ancho fijo de la regla, lo que es contrario a las limitaciones clásicas que se imponen al problema (Cap. VI - 1).

La aparición frecuente de métodos para trisectar ángulos pone de relieve el hecho de que matemáticos y profesores aún no han logrado difundir la realidad sobre el problema de la trisección, es decir, que este problema tiene fácil solución por métodos no clásicos, pero que no puede resolverse sujeto a las restricciones clásicas.

Hay muchas otras construcciones no clásicas para resolver el problema de la trisección (Bibliografía Nº 55). Varias de éstas se valen de curvas, tales como el gráfico de

$$x^3 + xy^2 + ay^2 - 3ax^2 = 0,$$

(Fig. VI-5) que no pueden construirse empleando únicamente regla y compás. La curva de la figura VI-5 se denomina la Trisectriz de Maclaurin y puede usarse para triscetar cualquier ángulo. Dada una Trisectriz de Maclaurin y cualquier ángulo ABC, trácese una recta m por el punto (2a, 0) que forme un ángulo igual al ángulo dado en el eje positivo de las x. Encuéntrense las tres intersecciones P_1, P_2, P_3 de la recta m con la curva dada. Una de las rectas P_iO, donde O es el origen, forma un ángulo con el eje positivo de las x igual a un tercio del ángulo dado. No es difícil determinar cuál de las tres rectas P_iO debe usarse, ya que se puede

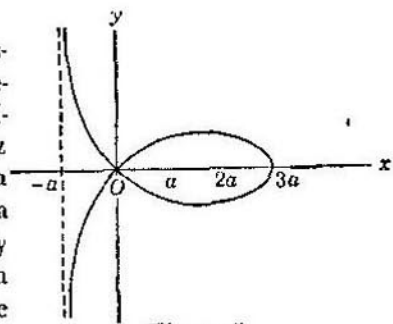


Fig. VI-5

comparar rápidamente tres veces cada uno de los tres ángulos obtenidos con el ángulo dado. Este método de trisectar ángulos se trata en muchos textos de geometría analítica. No se atiene a las limitaciones clásicas impuestas al problema en cuanto emplea una curva que no puede construirse usando únicamente regla y compás.

Ya hemos considerado varias construcciones no clásicas para resolver el problema de la trisección y hemos hecho notar la forma en que cada método contraviene las restricciones clásicas impuestas sobre el problema. En la sección siguiente estudiaremos unos cuantos trisectores mecánicos.

EJERCICIOS

1. Valiéndose de la construcción de Arquímedes y del Ejercicio 22, Cap. VI-2, encontrar un método para trisectar ángulos de cualquier medida.

2. Dibujar ángulos de aproximadamente 80°, 150°, 250°, 300° y 350°. Trisectar cada uno de los ángulos que se acaba de dibujar.

3. Describir e ilustrar la solución no clásica de Pappus del problema de la trisección, utilizando regla, compás, y la construcción de una hipérbola (Bibliografía Nº 55; págs. 22-23).

VI-8 TRISECTORES DE ANGULO MECANICOS. Hay varias clases de trisectores mecánicos de ángulo que varían en complejidad desde la tapa de una lata de café con dos varillas prendidas (Bibliografía Nº 4) hasta los polígonos articulados (sistemas de varillas unidas entre sí por ejes de articulación) en cuya construcción hay que efectuar mediciones muy cuidadosas.

El trisector de ángulo sencillo que citamos anteriormente puede hacerse con cualquier disco circular. Es una variante del tomahawk* (Bibliografía Nº 55; pág. 37). Sea r el radio del disco y O el centro. Prendase firmemente al disco, una varilla OPQ de longitud $2r$. En seguida prendase una segunda varilla PT tangente al disco en P (Fig. VI-6). Este invento puede usarse para trisectar cualquier ángulo dado ABC resbalando TP por B hasta que el disco esté tangente a un lado del ángulo dado, digamos en E, y Q se encuentre en el otro lado (Fig. VI-7). Los triángulos rectán-

*Especie de hacha de los indios (EE. UU.). N. de la T.

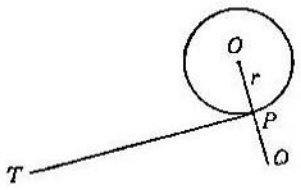


FIG. VI-6

gulos *QBP*, *OBP* y *OBE* son congruentes, luego las rectas *BP* y *BO* trisectan el ángulo dado.

Un sencillo trisector de ángulos hecho de cuatro varillas de madera (Bibliografía Nº 5) está basado en la construcción de Arquímides (Cap. VI-7). Otro tipo de trisector de ángulo, el isoclinóstato de Sylvester (Fig. VI-8) consiste en cuatro varillas *(OA, OC, OE y OG)* sujetas juntas por un eje en uno de sus extremos y unidas por un sistema de varillas más cortas que mantienen iguales a los ángulos formados por las varillas largas (Ejercicios 1, Cap. VI-9). Debido a que este tipo de mecanismo podía usarse para dividir un ángulo en cualquier número de partes iguales se denominó "isoclinóstato". Se puede colegir la procedencia de la idea original de Sylvester para este mecanismo de la cita siguiente extraída del título del impreso en que se publicó por primera vez: "Sobre el Abanico de una Dama, . . .".

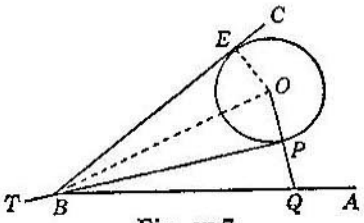


Fig. VI-7

Otro trisector de ángulo (polígono articulado) fue inventado por un abogado de Londres, Alfredo Bray Kempe, en 1877. Kempe se interesó en estos mecanismos después de oír la conferencia de Sylvester sobre este tema. Su trisector de ángulo (Fig. VI-9) se basa en el uso de paralelógramos invertidos (cuadriláteros de lados opuestos iguales y con un par de lados opuestos que se cruzan entre sí) semejantes,

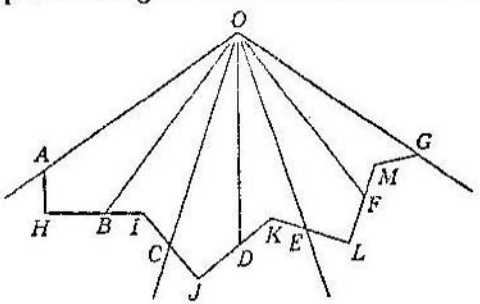


FIG. VI-8

$$ABCD \sim ADEF \sim AFGH,$$

y puede usarse para cualquier ángulo menor que una revolución completa.

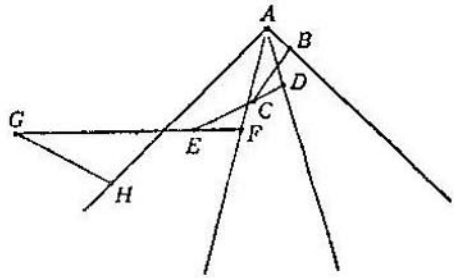


FIG. VI-9

Hasta aquí hemos demostrado que el problema de la trisección clásica es imposible y hemos visto que empleando un transportador, un polígono articulado, una regla marcada, una curva adecuada, etc., el problema de la trisección puede resolverse fácilmente por métodos no clásicos. La sección siguiente contiene un estudio más general sobre polígonos articulados.

VI-9 POLIGONOS ARTICULADOS. Un polígono articulado puede definirse como un sistema de varillas unidas por ejes de articulación con el objeto de permitir movimientos articulados sin que se produzcan deslizamientos. Entre 1860 y 1895 se hicieron muchos trabajos relacionados con estos mecanismos. James Watt no estaba satisfecho con el mecanismo empleado en la máquina a vapor para transformar el movimiento en línea recta del pistón en movimiento circular de las ruedas. Esta y otras consideraciones más fundamentales llevaron a una serie de intentos para construir una línea teóricamente recta. Esta recta (la inversa de una circunferencia con respecto a un punto sobre ella) fue lograda por fin por Peaucellier en 1864 e independientemente por Lipkin en 1871 (Bibliografía Nº 25). Bricard obtuvo otra solución en 1895. El rápido desarrollo y popularidad del tema se manifiesta en que de veintiséis trabajos presentados a la Asamblea General Anual de la Sociedad Matemática de Londres el 11 de noviembre de 1875, seis eran sobre polígonos articulados. Probablemente este desarrollo alcanzó su cima en 1876 cuan-

do Alfred Bray Kempe presentó a la Sociedad Matemática de Londres un trabajo "Sobre un Método General de describir Curvas Planas de grado n-ésimo por medio de manipulaciones con polígonos articulados", donde se explica la construcción de un polígono articulado que sirve para trazar cualquiera curva plana $f(x,y) = 0$ de grado n-ésimo. En consecuencia, teóricamente, puede dibujarse por medio de estos mecanismos el gráfico de cualquier curva polinomia plana. Sin embargo, si damos un vistazo a algunos de los diagramas de polígonos articulados para las curvas de grados más altos (Bibliografía Nº 45), veremos que se complican demasiado para ser útiles al respecto. También se ha demostrado (Bibliografía Nº 2; pág. 52) que ninguna curva trascendente, puede dibujarse por medio de polígonos articulados. Ultimamente, poco se habla de ellos, con la excepción de unos cuantos artículos que los recomiendan como ayudas visuales (Bibliografía Nº 36 y Nº 41) o como materia de interés general (Bibliografía Nº 25 y Nº 55).

Sin embargo, la actual falta de publicidad sobre estos mecanismos no significa que estén fuera de uso. En efecto, se han descubierto muchas aplicaciones de ellos y se usan mucho. Una descripción de los computadores, en cuya construcción se usa polígonos articulados, inventados en el Laboratorio de Radiación durante la Segunda Guerra Mundial, completa un libro de tamaño considerable. El pantógrafo (Ejercicio 4, Fig. VI - 10) se emplea para copiar figuras (figuras semejantes) y para el trazado de puntos equipotenciales en un campo eléctrico. El mecanismo que emplean algunos funcionarios públicos para firmar muchos cheques simultáneamente es una forma de polígono articulado. Casi todas las maquinarias contienen polígonos articulados —en forma manifiesta o disimulada— como puede verificarse fácilmente consultando cualquier texto sobre mecanismos. Desde el punto de vista del profesor, los polígonos articulados pueden servir mucho para mostrar a los estudiantes que la geometría no es solamente estática sino también dinámica (Bibliografía N.os 36 y 41).

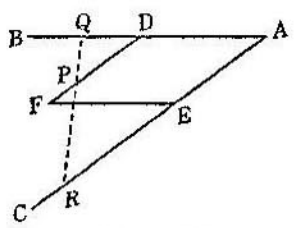


FIG. VI-10

Los polígonos articulados dieron origen a sólo uno de los varios

métodos de construcción no clásica. Concluiremos este capítulo con una breve discusión general sobre las construcciones clásicas y no clásicas.

EJERCICIOS

1. Dados los puntos A, B, C, D, E, F, G, en la Fig. VI-8 que se encuentran en una circunferencia de centro O, demostrar que $\angle AOC \cong \angle COE \cong \angle EOG$ si $AH \cong HB \cong CJ \cong JD \cong EL \cong LF$ y $BI \cong IC \cong DK \cong KE \cong FM \cong MG$, en donde AH, HI, IJ, JK, LM y MG, son, cada una, una sola varilla.

2. Dibujar un polígono articulado que divida a cualquier ángulo dado en cinco partes iguales.

3. Dar dos ejemplos del empleo de polígonos articulados para ilustrar propiedades matemáticas dinámicas (en contraposición con propiedades estáticas) en relación con figuras geométricas.

4. Se puede construir un pantógrafo con dos varillas largas AB, AC y dos cortas $FD \cong AE$, unidas como en la Fig. VI-10 de tal modo que $AD \cong FE$. Supongamos que se mantiene fijo el punto Q sobre AB y demuéstrese que a medida que P traza cualquier figura, R traza una figura semejante, siendo P, Q, R colineales, es decir, demostrar que la razón QP/QR es constante.

VI-10 RESUMEN. Los tres famosos problemas de construcción (Cap. VI-6) se formularon (Bibliografía Nº 2; pág. 20) en una época tan antigua como el siglo V a. C. Durante aquel mismo siglo, Hipias de Elis ideó una solución no clásica del problema de la trisección empleando la cuadratriz. Unos pocos años más tarde esta misma curva se empleó para resolver el problema de la cuadratura de un círculo. También se empleó la concoide en la trisección de un ángulo y en la duplicación de un cubo. Hacia fines del siglo III a. C., estos tres problemas famosos podían resolverse mediante métodos no clásicos. Los matemáticos griegos alcanzaban la cúspide de su desarrollo; Euclides desarrollaba los fundamentos de nuestra geometría plana y comenzaba a levantarse la geometría como ciencia. Sin embargo, los matemáticos tuvieron que esperar más de dos mil años para que el álgebra y la geometría se desenvolvieran lo suficiente para demostrar que los tres famosos problemas de construcción no podían resolverse utilizando únicamente regla y compás.

A los matemáticos griegos antiguos les parecía que todas las construcciones de geometría elemental debían hacerse empleando

únicamente regla y compás. Es así como estas construcciones clásicas han desempeñado un papel importante en el desarrollo de la geometría. En cierto sentido ellas son las precursoras de la geometría proyectiva. En el siglo X, un matemático árabe consideró construcciones con regla y compás con una abertura fija. Mucho más tarde (siglo XIX) Poncelet y también Steiner demostraron que las construcciones con regla y compás eran exactamente equivalentes a las construcciones con regla y un círculo fijo (Bibliografía Nº 2; pág. 30). En 1672 Georg Mohr y hacia 1800 Lorenzo Mascheroni demostraron que se necesitaba únicamente compás para obtener cualquier punto que pudiera construirse con regla y compás. En seguida comenzó a desarrollarse la geometría analítica y en el siglo XIX Gauss pudo obtener un criterio analítico para determinar la posibilidad de construir polígonos regulares. Otros descubrieron que no se podían construir las raíces de las ecuaciones que resultan de los tres problemas de construcción famosos, y por consiguiente estos problemas no podían resolverse empleando únicamente regla y compás.

Los polígonos articulados se desarrollaron rápidamente durante la última parte del siglo XIX. Pronto se demostró (Cap. VI - 9) que toda curva algebraica, y en particular una línea recta, podía trazarse empleando polígonos articulados. Desde aquella época y continuando en el siglo actual, Félix Klein contribuyó grandemente —gracias a sus famosas conferencias— a nuestro conocimiento de casi todas las materias a que nos hemos referido anteriormente.

En este capítulo hemos considerado las construcciones clásicas con regla y compás en forma detallada (Cap. VI - Secciones 1 a 6). Nos hemos referido también a algunos métodos usados en construcciones no clásicas (Cap. VI - Secciones 7 a 9). Para trisectar ángulos arbitrarios dados pueden emplearse marcas sobre una regla o curvas dadas adecuadas. Se pueden emplear polígonos articulados en una gran variedad de construcciones. Es posible inscribir en un círculo dado un polígono regular de cualquier número finito de lados utilizando un transportador. Algunos inventos como los que se acaban de citar nos permiten resolver problemas que no pueden resolverse por métodos clásicos. Otros aparatos de uso corriente como compases de división, reglas paralelas, cuadrado fijo, círculo fijo, permiten simplemente abreviar la construcción de

algún problema clásico sin hacer posible la resolución de ningún problema más. En general, cualquier problema de construcción tiene solución si no se imponen restricciones en los métodos que se pueden emplear; algunos problemas de construcción no pueden resolverse (Teorema VI - 1) si se emplea únicamente regla y compás. En consecuencia, hemos aprovechado los resultados obtenidos por Gauss, Klein y otros, hemos estudiado muchas construcciones clásicas corrientes, hemos desarrollado un criterio algebraico para determinar si se puede o no efectuar una construcción dada usando únicamente regla y compás, hemos aplicado este criterio a varios problemas clásicos, hemos estudiado unas cuantas construcciones no clásicas, y nos hemos referido brevemente a algunas aplicaciones modernas de estos métodos en la enseñanza y en la industria.

Hemos insistido en los problemas de construcción clásica famosos (Cap. VI - 6) y especialmente en el problema de la trisección. Nos hemos servido de este problema para ilustrar la aplicación de los métodos algebraicos en la solución de los problemas de construcción clásica. Hemos visto que mediante las teorías algebraicas se puede demostrar que son inútiles inevitablemente todos los intentos para obtener una solución clásica. Esta aplicación de las teorías algebraicas a las construcciones geométricas ofrece un ejemplo de la interdependencia entre el álgebra y la geometría. El capítulo que queda brinda otro ejemplo de esta interdependencia por medio del estudio de las representaciones gráficas de ciertas funciones algebraicas comunes.

EJERCICIOS

1. Construir polígonos regulares de 6, 7, 8 y 9 lados.
2. Especificar cuáles de los siguientes conjuntos de números contienen únicamente números susceptibles de construirse conforme a las restricciones clásicas: enteros, números racionales, números algebraicos, números reales.
3. Repetir el Ejercicio 2 para números que sean susceptibles de construirse empleando polígonos articulados.
4. Describir tres máquinas modernas en que se utilicen polígonos articulados.
5. Describir los polígonos articulados de tres instrumentos o máquinas comunes que usted haya empleado.
6. Discutir la contribución de Gauss al estudio de las construcciones.

CAPITULO VII

Representaciones gráficas

En la geometría euclidiana es posible representar los números enteros, los números racionales, los números constructibles (Cap. VI - 4), los números reales (Cap. I - 12) como puntos sobre una recta. Los números complejos pueden considerarse como pares ordenados de números reales (Cap. I - 15) y representarse como puntos en un plano de la geometría euclidiana. Cualquiera función uniforme de una variable real x sirve para obtener pares ordenados de números que pueden representarse gráficamente. El presente estudio de los conceptos algebraicos interpretados mediante conceptos geométricos se basa sobre estas representaciones. En este capítulo trataremos principalmente gráficos de funciones algebraicos con coeficientes reales en espacios (reales) euclidianos. Estudiaremos los gráficos de varios tipos de funciones, diferentes métodos de trazar gráficos y varias aplicaciones de los gráficos y de los métodos gráficos.

VII-1 LOS ESPACIOS EUCLIDIANO Y COMPLEJO. En el Capítulo VI nos servimos de la correspondencia biunívoca (Axioma de Cantor-Dedekind, Cap. I - 12) entre el conjunto de puntos sobre una recta en la geometría euclidiana y el conjunto de los números reales para la interpretación geométrica de las cuatro operaciones racionales. Estos conceptos pueden servir para establecer un isomorfismo (Cap. I - 8) entre el conjunto de puntos sobre una recta en la geometría euclidiana y el conjunto de los números reales. También existen isomorfismos entre pares de números reales y el conjunto de puntos sobre

un plano euclidiano, entre triples de números reales y el conjunto de puntos en el espacio euclidiano tridimensional y, en general, entre n-tuplos de números reales y el conjunto de puntos en el espacio euclidiano n-dimensional.

De acuerdo con los isomorfismos citados, cualquier punto sobre una recta en la geometría euclidiana puede identificarse unívocamente por un número real (coordenada); cualquier punto sobre un plano euclidiano puede identificarse por dos coordenadas reales; cualquier punto sobre un espacio euclidiano tridimensional por tres coordenadas reales, ..., y cualquier punto en un espacio euclidiano de n dimensiones por n coordenadas reales. En consecuencia, en la geometría de Euclides hablaremos de una recta como de un espacio unidimensional, hablaremos de un plano como de un espacio bidimensional, y, en general, estudiaremos espacios euclidianos n-dimensionales para cualquier entero positivo n.

También suele ser conveniente referirse a un conjunto de puntos que pueden hacerse isomorfos con el conjunto de los números complejos, como a un espacio complejo unidimensional. Ya que un número complejo puede considerarse como un par ordenado de números reales, un espacio complejo unidimensional es isomorfo con un plano euclidiano. Análogamente, un espacio con dos coordenadas complejas es isomorfo con un espacio euclidiano tetradimensional. En general, un espacio complejo n-dimensional es isomorfo con un espacio euclidiano $2n$-dimensional.

En nuestras breves descripciones anteriores de los espacios euclidianos y complejos no hemos considerado explícitamente relaciones métricas o de distancia. En un tratamiento completo habría que incluir las relaciones de distancia al establecer los isomorfismos citados anteriormente.

Cualquiera función de n variables que se anula para uno o más conjuntos de valores reales de las variables (n-tuplos reales) tiene un gráfico en un espacio (real) euclidiano n-dimensional, es decir, el conjunto de todos los puntos con coordenadas (n-tuplos) que hacen la función igual a cero. La función $x^2 + y^2 - 1$ representa el gráfico de un círculo de radio unidad en torno al origen en el plano euclidiano xy. La función $x^2 + y^2 + 1$ no tiene ceros reales y se dice que tiene un *gráfico vacío* en el plano xy. En consecuencia, una función polinomia en n variables puede o no puede tener

un gráfico no vacío en el espacio euclidiano de n dimensiones (Cap. VII - 2).

La situación es completamente diferente en un espacio con coordenadas complejas. Todo polinomio $f(x)$ con coeficientes complejos y grado positivo tiene un gráfico en un espacio con una coordenada compleja (Teorema IV - 3). Por ejemplo, $x^2 - 1$ tiene por gráfico a los puntos $+1$ y -1, sea que se considere que los puntos están en una recta real o en un espacio con una coordenada compleja similar a la estudiada en el Cap. I - 16; $x^2 + 1$ tiene un gráfico vacío sobre la recta real pero los puntos i y $-i$ son su gráfico en un espacio con una coordenada compleja. Esta propiedad de los polinomios $f(x)$ puede ampliarse (Ejercicios 4, 5 y 6) para demostrar que toda función algebraica de n variables tiene un gráfico no vacío en un espacio con n coordenadas complejas.

EJERCICIOS

1. Dar ejemplos de cuatro funciones de tres variables a) que tengan un gráfico no vacío en E_3; b) que tengan un gráfico vacío en E_3.
2. Dar ejemplos de tres funciones en n variables, a) que tengan un gráfico no vacío en E_n; b) que tengan un gráfico vacío en E_n.
3. Demostrar que cualquier polinomio en una variable con coeficientes complejos tiene un gráfico no vacío en un espacio con una coordenada compleja.
4. Demostrar que cualquier polinomio en n variables con coeficientes complejos tiene un gráfico no vacío en un espacio con n coordenadas complejas.
5. Demostrar que cualquiera función algebraica en una variable con coeficientes complejos tiene un gráfico no vacío en un espacio con una coordenada compleja.
6. Demostrar que cualquiera función algebraica de n variables con coeficientes complejos tiene un gráfico no vacío en un espacio con n coordenadas complejas.

VII - 2 POLINOMIOS. Cualquier polinomio lineal en n variables con coeficientes reales tiene siempre un gráfico real en un espacio E_n euclidiano n-dimensional. Este gráfico es un punto en E_1, una recta en E_2, un plano en E_3, y en general, un hiperplano en E_n. En consecuencia, el gráfico de una función lineal real de n variables es un E_{n-1} en E_n para todos los valores positivos de n. Cada uno de estos gráficos, E_{n-1} espacios, dividen al E_n correspondiente en dos regiones, en una de las cuales la función es positiva y en la

otra negativa. Los gráficos se llaman subespacios lineales y desempeñan un papel importante en muchas teorías matemáticas avanzadas.

Dada cualquiera ecuación lineal en n variables ($n > 1$) con coeficientes reales, se pueden encontrar mediante operaciones racionales muchos n-tuplos reales arbitrarios de números para los cuales la ecuación se satisface. En consecuencia, se pueden encontrar las coordenadas de muchos puntos arbitrarios sobre el gráfico mediante operaciones racionales. El gráfico queda totalmente determinado por n-tuplos (puntos) linealmente independientes (Cap. v - 13). Por ejemplo, un plano está completamente determinado por tres puntos que no se encuentran sobre la misma recta (Cap. v - 14) y, en general, un E_{n-1} está completamente determinado por n puntos que no se encuentran en el mismo E_{n-1}. Cuando los coeficientes de las n variables y el término constante son reales y diferentes de cero, los n puntos reales y distintos, es decir, las intersecciones del gráfico con los ejes coordenados determinan completamente el gráfico.

Cualquier polinomio de grado n en una variable con coeficientes complejos tiene n ceros complejos (Teorema iv - 2). Un polinomio de grado n con coeficientes reales tiene n ceros complejos pero puede o no puede tener ceros reales, como se ilustró en los ejemplos $x^2 - 1$, $x^2 + 1$ citados anteriormente. Por consiguiente, una ecuación polinomia real en una variable puede o no puede tener un gráfico no vacío sobre la recta real. Por medio de exactamente el mismo razonamiento, resulta que un polinomio real en dos variables puede o no puede tener ceros reales correspondientes a un valor dado de una de las variables. Por ejemplo, $x^2 + y^2 - 25$ tiene ceros $+3$ y -3 para $x = 4$, pero no tiene ceros reales para $x = 6$. Si un polinomio tal como $x^2 + y^2 + 1$ no tiene ceros reales para cada valor real de x, tiene un gráfico vacío en el plano euclidiano. En general, si un polinomio en n variables no tiene ningún cero real para cada conjunto real de valores de $n - 1$ de las variables, tiene un gráfico vacío en el espacio euclidiano de n dimensiones.

El gráfico de un polinomio divide al espacio en dos regiones en las cuales el polinomio tiene signo constante, dado que cualquier polinomio es una función continua de sus variables. Un polinomio en una variable cambia de signo si y sólo si la variable

pasa por un cero de multiplicidad impar (Cap. IV - 13). Para dos o más variables debe considerarse la trayectoria del punto general $(x_1, x_2, \ldots, x_n)$ al pasar por un punto sobre el gráfico de $f(x_1, x_2, \ldots, x_n)$. Por ejemplo, el polinomio $x^2 + y^2 - 1$ cambia su signo en $(1, 0)$ a medida que el punto (x, y) cruza la recta $y = 0$, pero no cambia su signo $(1,0)$ a medida que el punto (x, y) cruza la recta $x = 1$. En general, la multiplicidad m de un punto de intersección P de una curva C con el gráfico de un polinomio en n variables puede definirse estableciendo que a medida que el punto $(x_1, x_2, \ldots, x_n)$ cruza la curva C, el polinomio cambia de signo en P, si y sólo si m es impar. Definiremos solamente la multiplicidad de la intersección de una recta y una curva polinomia en un plano.

Supongamos que una curva polinomia dada $f(x', y')$ y una recta dada se cortan en un punto $P:(s, t)$ con una multiplicidad k, en que k debe determinarse. Por medio del cambio de variables (traslación, Cap. V - 15) $x = x' - s, y = y' - t$, la curva $f(x + s, y + t) = g(x, y)$ y la recta dada expresada en las nuevas coordenadas se cortan en el nuevo origen con la misma multiplicidad k con que la curva $f(x', y')$ cortaba a la recta dada en P. La ecuación de la recta tiene ahora la forma $y = mx$ o bien la forma $x = 0$. Después de sustituir en estos dos casos consideremos, respectivamente, los polinomios $g_1(x) = g(x, mx)$ y $g_2(y) = g(0, y)$. El valor de k queda entonces determinado por el hecho de que los términos de menor grado en $g_1(x)$ tienen grado k; o si la recta es $x = 0$, $g_2(y)$ tiene grado k. Conforme a esta definición, se dice que una recta y una curva que no pasan las dos por el punto P, tienen una *intersección de multiplicidad cero* en P.

El gráfico de un polinomio en n variables divide a un espacio euclidiano n-dimensional en un número finito de regiones, en cada una de las cuales el polinomio tiene signo constante. El problema general de determinar estas regiones [las soluciones de $0 < f(x_1, x_2, \ldots, x_n)$ y $0 < -f(x_1, x_2, \ldots, x_n)$] y sus límites [las soluciones de $0 = f(x_1, x_2, \ldots, x_n)$] aún no ha sido completamente resuelto. No obstante, se ha hecho una considerable cantidad de trabajo con polinomios en dos o tres variables. En particular, estudiaremos ahora polinomios reales de grado dos en dos variables (Cap. VII - 3) y polinomios reales de grado dos en tres variables (Cap. VII - 4).

EJERCICIOS

1. Escribir una ecuación lineal en n variables reales y encontrar un conjunto de n puntos que determinen su gráfico cuando n es igual a a) 2; b) 3; c) 4; d) 5; e) 6; f) 10.

2. Encontrar la multiplicidad de la intersección en el origen de la recta $y = 0$ con cada una de las siguientes curvas:

(a) $y = x^3$,
(b) $x = y^3$,
(c) $y^4 = x^2$,
(d) $x^3 + 3x^2y + x^2 = 0$,
(e) $x^2 + y^2 = 1$,
(f) $x = 0$

3. Encontrar la multiplicidad de la intersección en el origen de cada una de las siguientes rectas con cada una de las curvas del Ejercicio 2: a) $x = 0$; b) $y = x$.

4. Encontrar la multiplicidad de la intersección en (2, 1) de la recta $y = 1$ con cada una de las siguientes curvas:

(a) $x + y = 3$,
(b) $x^2 + y^2 = 5$,
(c) $x = 2y^2$,
(d) $(x - 2)^2 + y^2 = 1$,
(e) $x^3 = 8y$,
(f) $x^2 - 3y^2 = 1$

5. Repetir el Ejercicio 4, empleando cada una de las siguientes rectas: a) $x = 2$; b) $x = 2y$.

VII-3 SECCIONES CONICAS. La ecuación cuadrática general real en dos variables tiene la forma

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0, \tag{VII-1}$$

donde se supone que los coeficientes son reales y que $A^2 + B^2 + C^2 \neq 0$. Los gráficos de las ecuaciones de la forma (VII-1) se denominan *secciones cónicas*, dado que para cada conjunto de coeficientes reales para los cuales (VII-1) tiene un gráfico no vacío, el gráfico puede obtenerse por medio de la intersección de un plano y un cono circular recto (posiblemente degenerado). En esta sección estudiaremos brevemente el desarrollo de la hipérbola, de la parábola, de la elipse y del círculo como intersecciones de planos con un cono recto circular, es decir, como secciones planas de un cono recto circular. También mencionaremos varias propiedades de estas secciones cónicas a manera de repaso de geometría analítica.

Un círculo puede definirse como el lugar geométrico de los puntos de un plano que equidistan de un punto fijo dado Q del

plano. Si hay un sistema de coordenadas (x,y) y una relación de distancia en el plano, el círculo es el gráfico de un polinomio $(x - h)^2 + (y - k)^2 - r^2$, en que su centro Q tiene coordenadas (h, k) y la distancia es $r \leqq 0$. Un círculo con $r = 0$ se denomina *círculo punto* y se clasifica como una forma degenerada del círculo.

Consideremos un círculo real no degenerado con centro Q y sea $P \neq Q$ un punto fijo real arbitrario sobre la recta que pasa por Q y es perpendicular al plano del círculo. El lugar geométrico de los puntos del conjunto de rectas que unen a P con los puntos del círculo se denomina un *cono recto circular* (Fig. VII - 1). El cono tiene dos *mantos* que se juntan en P. El lugar geométrico de los puntos del conjunto de rectas perpendiculares al plano del círculo a través de los puntos del círculo se denomina *cilindro circular recto* (Fig. VII - 2) y puede considerarse como el caso límite del cono a medida que la distancia PQ crece indefinidamente.

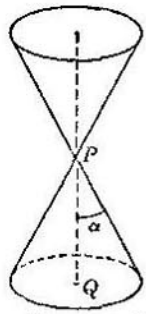


FIG. VII - 1

FIG. VII - 2

Sea π un plano real arbitrario y consideremos como anteriormente el cono circular recto generado por rectas que pasan por el punto fijo P y un círculo no degenerado dado con centro Q. Sea α el ángulo constante entre las rectas generatrices y PQ. Se dice que un gráfico de la ecuación cuadrática (VII - 1) es degenerado si y sólo si resulta de hacer pasar el plano π a través de P. Esta condición puede también expresarse algebraicamente como sigue (Bibliografía Nº 18; págs. 215-219): El gráfico es degenerado si y sólo si $\Delta = 0$, en que

$$\Delta = \begin{vmatrix} 2A & B & D \\ B & 2C & E \\ D & E & 2F \end{vmatrix}.$$

Gráficos no degenerados de (VII - 1) son una hipérbola, una parábola o una elipse según que $B^2 - 4AC > , =, < 0$. Geométricamente, estos tres casos se generan, respectivamente, según que el menor ángulo θ entre el plano π y la recta PQ sea $<, =, > \alpha$ (Fig. VII - 3). (La normal al plano forma un ángulo con PQ igual al complemento de θ). Por ejemplo, consideremos el cono $3x^2 + 3y^2 - z^2 = 0$, con $\alpha = 30°$. Para cualquier número real k el plano $z = k$, con θ igual a un ángulo recto, corta al cono en un círculo $3x^2 + 3y^2 - k^2 = 0$; el plano $z = x + k$ con $\theta = 45° > \alpha$ corta al cono en una elipse $2x^2 + 3y^2 - 2xk - k^2 = 0$; el plano $z = x\sqrt{3} + k$ con $\theta = 30° = \alpha$ corta al cono en una parábola $3y^2 - 2xk\sqrt{3} - k^2 = 0$; y el plano $x = 2x + k$ con $\theta < \alpha$ corta al cono en una hipérbola $3y^2 - x^2 - 4xk - k^2 = 0$.

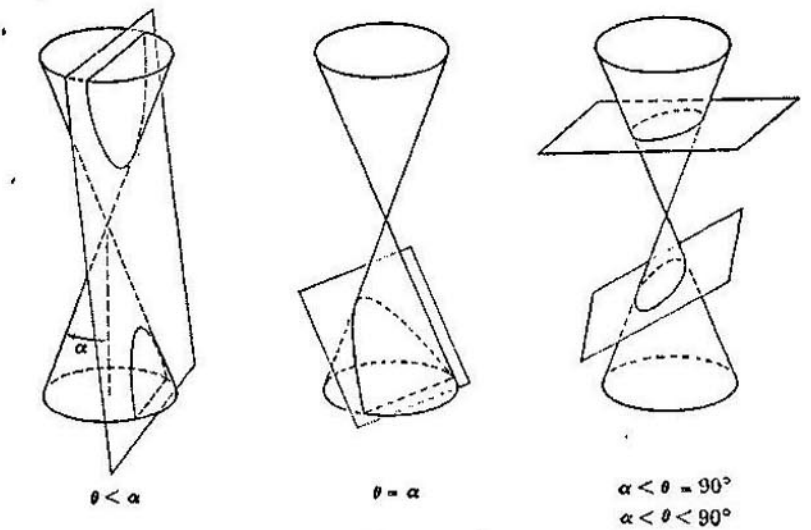


FIG. VII—3

Las cónicas degeneradas pueden identificarse algebraicamente o geométricamente. Desde un punto de vista geométrico (Ejercicio 1), una hipérbola puede degenerar en dos rectas que se cortan; una parábola en dos rectas coincidentes o en dos rectas paralelas (empleando un cilindro circular recto), y una elipse en un punto. La elipse se convierte en un círculo cuando θ es un ángulo recto.

En la mayoría de los textos de geometría analítica se demuestra (Ejercicio 6) que si los ejes coordenados efectúan una rotación

(Cap. V - 15) igual a un ángulo ψ, en que $\operatorname{tg} 2\psi = B/(A - C)$ si $A \neq C$ y $\psi = 45°$ si $A = C$, la ecuación (VII - 1) toma la forma

$$(VII - 2) \qquad A'x^2 + C'y^2 + D'x + E'y + F' = 0$$

También se puede demostrar (Ejercicio 7) que los números $A + C$, $B^2 - 4AC$, y Δ permanecen invariables al efectuarse una rotación o una traslación de los ejes coordenados (Bibliografía Nº 11; pág. 100). En consecuencia $B^2 - 4AC = -4A'C'$ y el gráfico, posiblemente degenerado, de (VII - 2) es una hipérbola, parábola, o elipse según que $A'C' <, =, > 0$. Ya que A' y C' no pueden ser ambas cero en la ecuación cuadrática (VII - 2), la ecuación general de una parábola no degenerada puede escribirse en una de las formas

$$(VII - 3) \qquad (y - k)^2 = 2p(x - h) \text{ ó } (x - h)^2 = 2p(y - k).$$

Análogamente, si $A'C' \neq 0$, se hace $h = -D'/2A'$ y $k = -E'/2C'$. Luego una elipse no degenerada tiene una ecuación de la forma:

$$(VII - 4) \qquad \frac{(x - h)^2}{a^2} + \frac{(y - k)^2}{b^2} = 1, \quad 0 < a, \quad 0 < b$$

y una hipérbola no degenerada tiene una ecuación de la forma

$$(VII - 5) \quad \frac{(x - h)^2}{a^2} - \frac{(y - k)^2}{b^2} = 1 \quad \text{o} \quad \frac{(y - k)^2}{a^2} - \frac{(x - h)^2}{b^2} = 1.$$

La primera parábola de (VII - 3) tiene eje $y = k$, vértice (h, k), y pasa por los puntos $(h + p/2, k \pm p)$. Se puede definir en el plano como el lugar geométrico de los puntos equidistantes de la recta $x = h - p/2$ (denominada la *directriz*) y del punto $(h + p/2, k)$ (llamado foco).

La elipse (VII - 4) tiene centro (h, k) y, si suponemos que $a^2 > b^2$, los extremos de su eje mayor se encuentran en $(h \pm a, k)$, los extremos de su eje menor se encuentran en $(h, k \pm b)$, y sus focos se encuentran en $(h \pm \sqrt{a^2 - b^2}, k)$. Si $a^2 = b^2$, es una circunferencia. La elipse puede definirse en el plano como el lugar geométrico de los puntos P tales que $PF_1 + PF_2 = 2a$, en donde F_1 y F_2 son los focos.

La primera hipérbola de (VII - 5) tiene el centro en (h,k), los extremos de su eje mayor en $(h \pm a, k)$, sus focos en $(h \pm \sqrt{a^2 + b^2}$

$k)$, y las asíntotas $b(x - h) = \pm a(y - k)$. Se puede definir en el plano como el lugar geométrico de los puntos P tales que $PF_1 - PF_2 = \pm 2a$.

En consecuencia el gráfico real (en caso de que exista) de una ecuación cuadrática general (VII - 1) puede obtenerse como la sección de un cono recto circular (posiblemente degenerado) interceptada por un plano y se denomina sección cónica. La forma del gráfico puede determinarse mediante la cantidad $B^2 - 4AC$ y la característica (Cap. V - 10) del determinante Δ. Se puede demostrar que las definiciones de hipérbola, parábola, y elipse como lugares geométricos en un plano son equivalentes a las definiciones como secciones de un cono recto circular. En (Bibliografía Nº 38; págs. 102-138) puede consultarse un estudio muy ameno de las secciones cónicas; en (Bibliografía Nº 18; págs. 171-236) puede consultarse un estudio más completo y en (Bibliografía Nº 11) una historia de las secciones cónicas y superficies cuádricas.

EJERCICIOS

1. Dibujar figuras que ilustren en qué forma pueden obtenerse cada una de las siguientes cónicas degeneradas no vacías como secciones planas de un cono recto circular o de un cilindro recto circular: a) dos rectas que se cortan; b) dos rectas coincidentes; c) dos rectas paralelas distintas; d) un punto.

2. Hacer el gráfico de las siguientes secciones cónicas:

(a) $x^2 + y^2 = 25$,
(b) $9x^2 + 4y^2 = 36$,
(c) $9x^2 - 4y^2 = 36$,
(d) $x^2 = y + 2$,
(e) $x^2 - 2x = y$,
(f) $x = y^2 - 2y + 5$,
(g) $y = x^2 - 6x + 7$.

3. Reconocer los gráficos de las ecuaciones siguientes:

(a) $x^2 - 2y^2 + 3x + y = 5$,
(b) $x^2 - 2xy + y^2 - 2x + y + 7 = 0$,
(c) $xy = 12$,
(d) $x^2 + 2xy + y^2 + 2x + 2y + 1 = 0$,
(e) $3x^2 + 2xy - y^2 + 5x - 2y + 1 = 0$,
(f) $x^2 + 2xy + y^2 + x + y - 6 = 0$,
(g) $2x^2 - xy + 3y^2 - 4x + 6y = 0$.

4. Escribir cada una de las ecuaciones del Ejercicio 3 en la forma (VII-2).

5. Hacer el gráfico de las secciones cónicas del Ejercicio 3.

6. Deducir la ecuación (VII-2) de la (VII-1) considerando el efecto de una rotación (Cap. V-15) sobre (VII-1), mostrando como debe elegirse un ángulo de

rotación tal que desaparezca el término xy, y expresando los nuevos coeficientes respecto de los coeficientes antiguos y del ángulo elegido.

7. Demostrar que cada una de las expresiones siguientes permanecen invariantes sometidas a la rotación empleada en el Ejercicio 6: a) $A + C$, b) $B^2 - 4AC$, c) Δ.

8. Encontrar la característica (Cap. V-10) del determinante Δ correspondiente a cada ecuación del Ejercicio 3. Examinar el significado general de la característica de Δ.

VII-4 SUPERFICIES CUADRICAS. El gráfico de una ecuación cuadrática $f(x,y,z) = 0$ en tres variables con coeficientes reales se denomina *superficie cuádrica*. Si falta una de las variables en la ecuación $f(x,y,z) = 0$, como ser, z, entonces $f(x, y,z)$ puede escribirse como $f(x,y)$ y el gráfico en tres dimensiones (superficie cuádrica) de la ecuación cuadrática $f(x,y) = 0$ corta a todo plano $z = c$ en una sección cónica (Cap. VII - 3) congruente con el gráfico de $f(x,y)$ en el plano xy. En este capítulo hablaremos indiferentemente del gráfico de $f(x,y) = 0$ y del gráfico de $f(x,y)$. Esta terminología es análoga a nuestras consideraciones anteriores respecto a las raíces de una ecuación polinomia $f(x) = 0$ y los ceros de un polinomio $f(x)$. El gráfico de $f(x,y)$ en tres dimensiones consiste en todos los puntos sobre rectas paralelas al eje z y que pasan por puntos del gráfico de $f(x,y)$ en el plano xy. El gráfico en tres dimensiones es un caso especial de un cilindro (no necesariamente circular). Estrictamente hablando, un *cilindro* puede definirse como una superficie que comprende todos los puntos sobre rectas que son paralelas a una recta fija y que pasan por puntos de una curva fija en un plano que no es paralelo a la recta fija. De esta manera el gráfico de cualquiera ecuación cuadrática real $f(x, y,z) = 0$ al que le falta una de las variables puede considerarse como un cilindro que tiene un eje coordenado x como recta fija y una sección cónica como curva fija en el plano coordenado que no contiene a la recta fija. Cualquier plano paralelo al plano de la curva fija corta al cilindro en una sección cónica congruente (por traslación) a la curva fija.

Supongamos que $f(x,y,z) = 0$ es cualquiera ecuación cuadrática real en tres variables x, y, z y que $mx + ny + rz + d = 0$ es el gráfico de cualquier plano real (Cap. VII - 2). Entonces por lo menos uno de los coeficientes m, n, r es diferente de cero, y existe una rotación en el espacio tal que en el nuevo sistema coordenado el

plano citado tiene la ecuación $z = c$ y la superficie cuádrica tiene la ecuación $g(x,y,z) = 0$, en que $g(x,y,z)$ es un polinomio cuadrático real. La intersección del plano y de la superficie cuádrica se encuentra ahora sobre el cilindro $g(x,y,c) = 0$ y, dado que $g(x,y,c)$ es un polinomio cuadrático real en x e y, esta intersección es una sección cónica. Encontramos así, por rotación del sistema coordenado en forma tal que el nuevo eje z sea perpendicular al plano dado, que cualquiera sección plana de una superficie cuádrica es una sección cónica. El gráfico de cualquier superficie cuádrica se puede obtener teniendo presente las secciones planas (secciones cónicas) paralelas a los planos coordenados. Por ejemplo $b^2x^2 + a^2y^2 = a^2b^2z$, siendo $ab \neq 0$ (Fig. VII - 4), tiene una sección elíptica en el plano $z = c$ para todos los valores positivos de c, tiene un punto para $c = 0$ y ningún gráfico real si c es negativo. Tiene una sección parabólica para todos los valores reales de d cuando $x = d$ ó $y = d$, y se denomina un paraboloide elíptico.

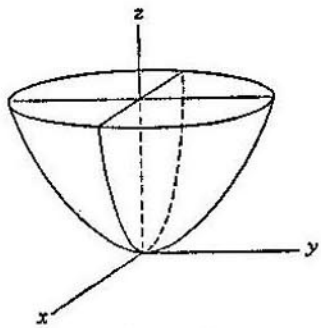


Fig. VII-4

El problema de obtener la superficie cuádrica de sus secciones planas paralelas a los planos coordenados es exactamente análogo a aquél de obtener una sección cónica de sus secciones lineales paralelas a los ejes coordenados. Por ejemplo, la parábola $y = x^2$ corta a toda recta $x = a$ en un solo punto y corta a la recta $y = b$ en dos puntos distintos cuando b es positivo, en dos puntos coincidentes cuando $b = 0$, y en dos puntos imaginarios (gráfico vacío en el plano euclidiano) cuando b es negativo. El gráfico de la parábola puede imaginarse gracias a estas intersecciones, teniendo presente el hecho de que el gráfico es continuo (Cap. III - 12 y Cap. III - 13). Este método de determinar gráficos puede emplearse para el trazado de curvas de nivel que representan puntos de la misma elevación en los mapas, para el trazado de líneas isotermas que representan puntos de la misma temperatura, y en muchas otras aplicaciones de curvas de niveles como se señala en algunos textos de cálculo. En consecuencia, dado cualquier polinomio $f(x,y)$, el problema de formarse una imagen de la superficie $z = f(x,y)$ de las secciones planas en las

cuales $z = c$, es el mismo que aquél de imaginar la topografía de un paisaje mientras se observa las curvas de nivel sobre un mapa.

El método de determinar gráficos mediante secciones puede emplearse también para formarse la imagen de gráficos de cuatro dimensiones. En este caso las secciones se eligen mediante paralelas tridimensionales a la coordenada tridimensional. Por ejemplo $x^2 + y^2 = 1$ puede representar el gráfico de un círculo de radio unidad en el plano xy o un cilindro en el espacio tridimensional de modo que toda sección que resulte de la intersección con un plano $z = c$, es un círculo de radio unidad. Análogamente, $x^2 + y^2 + z^2 = 1$ puede representar el gráfico de una esfera de radio unidad en un espacio tridimensional o un cilindro en un espacio tetradimensional tal que toda sección que resulte de la intersección con un espacio tridimensional $w = c$ es una esfera de radio unidad. Las limitaciones de este método aplicado al espacio de cuatro dimensiones, de cinco dimensiones, etc., residen en el hecho de que estamos habituados al espacio tridimensional y en la capacidad de formarse imágenes mentales que tenga la persona que utilice el método (Ejercicios 9 a 14).

Algunas superficies cuádricas tales como el hiperboloide de una hoja

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$$

(Fig. VII - 5), contienen líneas rectas y se denominan *superficies regladas*. Por ejemplo, consideremos los dos pares de planos

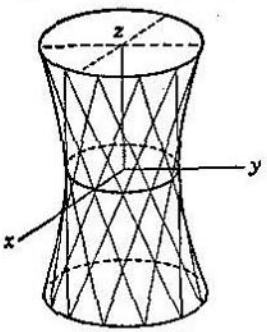


Fig. VII-5

$$\frac{x}{a} - \frac{z}{c} - k\left(1 + \frac{y}{b}\right) = 0,$$

$$1 - \frac{y}{b} - k\left(\frac{x}{a} + \frac{z}{c}\right) = 0$$

y

$$\frac{x}{a} + \frac{z}{c} - m\left(1 - \frac{y}{b}\right) = 0,$$

$$1 + \frac{y}{b} - m\left(\frac{x}{a} - \frac{z}{c}\right) = 0.$$

para todo valor real de k la intersección del primer par de planos es una recta sobre la superficie cuádrica,

$$\frac{x^2}{a^2} - \frac{z^2}{c^2} = 1 - \frac{y^2}{b^2},$$

que resulta al eliminar k entre las ecuaciones de los dos planos. De esta manera se obtiene una recta sobre la superficie cuádrica para cada valor real de k. Análogamente, se obtiene un segundo conjunto de rectas sobre la superficie cuádrica si se consideran valores reales de m en las ecuaciones del segundo par de plano. Cuando se emplean coeficientes y coordenadas complejas, toda cónica central (hipérbola o elipse) tiene un gráfico reglado. Los conos y los cilindros son ejemplos corrientes de superficies regladas en el espacio real tridimensional. Las superficies cuádricas reales pueden clasificarse en elipsoides, paraboloides elípticos, etc., en relación con los coeficientes de los términos de segundo grado y con el número de líneas de la superficie que pasan por cada punto de la superficie. La mayória de los textos de geometría analítica considera unas cuantas superficies cuádricas especiales. El propósito que nos guió en esta sección fue el de señalar que existe una teoría bastante compleja y una clasificación de las superficies cuádricas análogas a aquéllas de las secciones cónicas. Para mayores detalles se puede consultar los N.os 11, 16 y 18 de la Bibliografía.

EJERCICIOS

1. Dar un ejemplo de una ecuación cuadrática real general en tres variables.
2. Indicar las ecuaciones de cinco cilindros en el espacio de tres dimensiones que tengan diferentes tipos de curvas fijas.
3. Hacer el gráfico de las curvas fijas de los cilindros dados en el Ejercicio 2.
4. Hacer el gráfico de los cilindros dados en el Ejercicio 2.
5. Discutir las secciones que resultan en cada una de las siguientes superficies cuádricas por medio de todos los planos $z = c$:

(a) $4x^2 + 9y^2 + 4z^2 = 36$,
(b) $x^2 = 2y$,
(c) $x^2 - y^2 = 1$,
(d) $x^2 + y^2 = z^2$,
(e) $x^2 - z^2 = 0$,
(f) $x^2 - 4y^2 = 8z$.

6. Repetir el Ejercicio 5 para todos los planos $x = a$ e $y = b$.
7. Hacer el gráfico de las superficies cuádricas del Ejercicio 5.
8. Dar los nombres de las superficies cuádricas del Ejercicio 5.
9. Discutir el gráfico $x = 1$ en los siguientes espacios: a) el eje de las x; b) el plano xy; c) el espacio de tres dimensiones xyz; d) el espacio de cuatro dimensiones $xyzw$; e) el espacio de cinco dimensiones $xyzwv$.

10. Repetir el Ejercicio 9 para $x^2 - 1$.

11. Discutir los gráficos de $x^2 + y^2 = 4$ en los espacios b) hasta e) del Ejercicio 9.

12. Repetir el Ejercicio 11 para $y = x^2$.

13. Discutir los gráficos de las ecuaciones polinomias del Ejercicio 5 en el espacio de cuatro dimensiones $xyzw$.

14. Discutir los gráficos siguientes en un espacio de cuatro dimensiones:

(a) $x^2 + y^2 + z^2 + w^2 = 1$,
(b) $x + y + z + w = 1$,
(c) $x^2 + y^2 = z^2 + w^2$.

15. ¿Cuántas líneas de la superficie de un cono (Fig. VII-1) pasan por cada punto de ella?

16. ¿Cuántas líneas hay en cada punto de un cilindro (en un espacio de tres dimensiones) que tenga como curva fija a una sección cónica no degenerada?

17. Dada una ecuación cuadrática real general en tres variables (Ejercicio 1), escribir su determinante Δ análogo a aquel de la sección cónica general del Cap. VII-3.

18. Encontrar la característica de Δ de cada una de las superficies cuádricas de los Ejercicios 2 y 5. Hacer consideraciones sobre el significado general de la característica de Δ.

VII-5 CURVAS PLANAS DE GRADO SUPERIOR.

Los gráficos de polinomios $f(x,y)$ de grado mayor que dos en el plano xy se denominan *curvas planas de grado superior*. Estos gráficos se han clasificado perfectamente para los casos en que $f(x,y)$ tiene grado tres o cuatro, es decir, para las curvas cúbicas y cuárticas. Muchas otras curvas se han estudiado ampliamente. En esta sección definiremos un punto singular y, en particular, un punto doble. En seguida clasificaremos puntos dobles y por último clasificaremos curvas planas cúbicas en relación a sus puntos dobles. Se mencionarán algunas propiedades generales de las curvas planas de grado superior.

Se dice que un punto P de una curva, es un *punto singular* de ella si toda recta que pasa por P corta a la curva en P, con una multiplicidad (Cap. VII - 2) de por lo menos dos. Si alguna recta que pasa por un punto singular P corta a la curva con multiplicidad dos en P, entonces P es un *punto doble*. Cualquiera recta pertenece completamente a una curva (es decir, es una componente de ella) de grado n o bien corta a la curva en, a lo sumo, n puntos. Esto se puede demostrar resolviendo simultáneamente una ecua-

ción $f(x,y) = 0$ de grado n y la ecuación de una recta, pues la ecuación resultante en una variable es idénticamente nula o de grado, a lo sumo, n. Análogamente, dos curvas de grado m y n tienen una componente en común o se cortan en, a lo sumo, mn puntos. Empleando estos argumentos, se puede demostrar que una curva de grado n puede tener a lo sumo $\frac{1}{2}(n-1)(n-2)$ puntos dobles (Bibliografía Nº 23; págs. 41-42). En particular, una curva cúbica tiene a lo sumo un punto doble (Ejercicio 1).

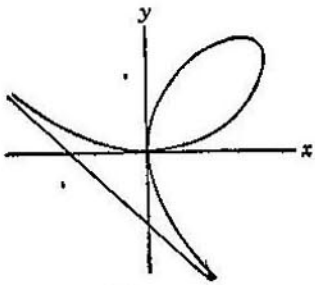


FIG. VII-6

En un punto cualquiera (no singular), una curva de grado n tiene una tangente única; en un punto doble, tiene dos tangentes; y en general, en un punto singular P tiene k tangentes si toda recta que pasa por P corta a la curva en P con multiplicidad por lo menos k, y alguna recta corta a la curva en P con multiplicidad exactamente k.

Los puntos dobles se clasifican en *nodos* si las tangentes son distintas, y *cúspides* si coinciden. Si las tangentes son rectas imaginarias conjugadas, el punto doble se denomina *punto aislado o acnodo*. El Folio de Descartes, $x^3 + y^3 = 3axy$ (Fig. VII - 6), tiene un nodo en el origen y la recta $x + y + a = 0$ es su asíntota (Cap. VII - 6); la parábola semicúbica $y^2 = x^3$ (Fig. VII - 7) tiene una cúspide en el origen; y la curva $y^2 = x^2(x - 1)$ (Fig. VII - 8) tiene un punto aislado en el origen.

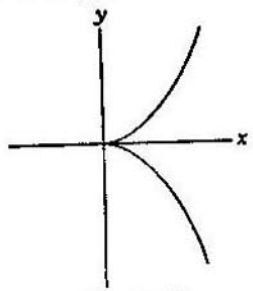


FIG. VII-7

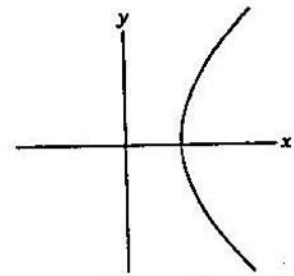


FIG. VII-8

Las curvas cúbicas se clasifican generalmente como sigue, teniendo en cuenta sus puntos dobles:

(i) Curvas cúbicas sin puntos dobles: *cúbicas elípticas;*

(ii) Curvas cúbicas con un nodo: *cúbicas nodales;*

(iii) Curvas cúbicas con una cúspide: *cúbicas cuspidales.*

Puede consultarse muchas propiedades de las curvas cúbicas en (Bibliografía Nº 23; págs. 139-243) y (Bibliografía Nº 26; págs. 201-263).

Se puede clasificar también a las curvas cuárticas en relación con sus puntos singulares. En Bibliografía Nº 23, págs. 244-328, y Nº 26, págs. 264-349, se puede consultar esta clasificación y muchas propiedades de las curvas cuárticas.

Las curvas planas de cualquier grado n pueden considerarse según sus puntos dobles y otros puntos singulares. En particular, cualquier curva irreducible (Cap. VII - 9) que tenga su número máximo de puntos singulares, es decir, *deficiencia cero,* se denomina *curva unicursal.* Una curva unicursal se caracteriza porque las coordenadas de todo punto de la curva pueden expresarse racionalmente por medio de un solo parámetro. Las curvas unicursales son importantes en varias teorías matemáticas.

Las dos secciones que siguen contienen mayores detalles sobre el trazado de curvas planas de orden superior.

EJERCICIOS

1. Demostrar que una curva cúbica irreductible tiene a lo sumo un punto doble.

2. Hacer un gráfico de cada una de las curvas siguientes e indicar la ecuación correspondiente a) cúbica elíptica; b) cúbica nodal; c) cúbica cuspidal.

VII - 6 FUNCIONES RACIONALES. Un polinomio $f(x, y)$ en x e y con coeficientes complejos puede considerarse como un polinomio en y con coeficientes pertenecientes al anillo de los polinomios en x con coeficientes complejos. La ecuación $f(x, y) = 0$ define, por consiguiente, a y como una *función algebraica* de x (Cap. III - 16). Si $f(x, y)$ es de grado n en y, hay exactamente n valores complejos de y para cada valor de x, de modo que el coeficiente de y^n no se anula. En consecuencia, una función algebraica no es, en general, uniforme para n mayor que uno. Para $n = 1$, tenemos $f(x, y) = p(x)y - q(x) = 0$, donde $p(x)$ y $q(x)$ son polinomios en x. En esta sección consideraremos el caso especial $y = q(x)/p(x)$, en que $p(x)$ y $q(x)$ son polinomios en x primos entre sí con coeficientes reales.

Estudiaremos en especial las asíntotas y las intersecciones con los

ejes coordenados. El gráfico (Fig. VII-9) de la ecuación $2x + 3y = 6$ tiene intersecciones con el eje x en 3 y con el eje y en 2. En general, cada intersección de una curva con un eje coordenado puede encontrarse valiéndose del origen y del punto unidad para determinar un segmento de longitud orientada igual a la coordenada del punto de intersección. Esta coordenada se denomina una *intersección* de la curva (con uno de los ejes coordenados). En particular, los ceros reales de una función $y = f(x)$ son las intersecciones de su gráfico con el eje x.

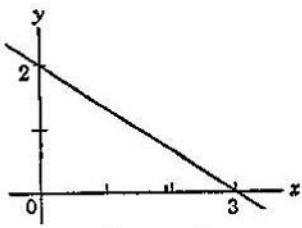


FIG. VII-9

Es fácil describir una asíntota. Supongamos que un punto variable P sobre el gráfico de $f(x,y)$ se mueve de modo que una o sus dos coordenadas se hagan indefinidamente grandes. Si al mismo tiempo el punto P se aproxima indefinidamente a una recta $ax + by + c = 0$, esta recta se denomina una *asíntota* del gráfico de $f(x,y)$. Por ejemplo $x^2y - 1$ tiene a ambos ejes coordenados como asíntotas (Fig. VII - 10); $xy - 2y - 1$ tiene a las rectas $x = 2$ e $y = 0$ como asíntotas (Fig. VII - 11). Las asíntotas de la forma $y = c$ se denominan *asíntotas horizontales;* aquellas de la forma $x = c$, *asíntotas verticales.* Existen también otras asíntotas como, por ejemplo, la recta $x + y + a = 0$ de la Fig. VII - 6.

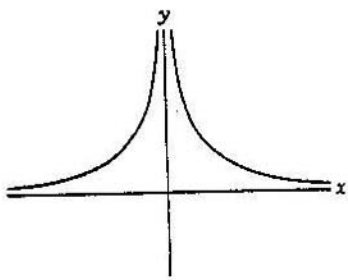


FIG. VII-10

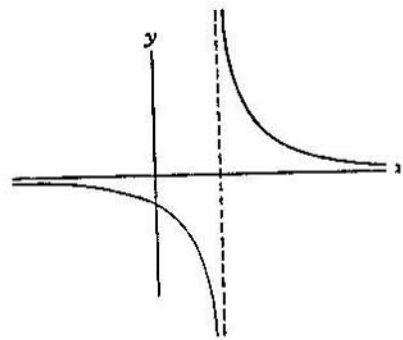


FIG. VII-11

Las asíntotas horizontales del gráfico de un polinomio $f(x,y)$ se obtienen igualando a cero los coeficientes de la más alta potencia

de x en $f(x, y)$. Análogamente, las asíntotas verticales pueden obtenerse igualando a cero los coeficientes de la más alta potencia de y. Por ejemplo, $xy - 2y - 1$ tiene una asíntota horizontal $y = 0$ y una asíntota vertical $x = 2$ (Fig. VII - 11).

La función $y = q(x)/p(x)$, en que $q(x)$ y $p(x)$ son polinomios en x, se denomina *función racional* de x (Cap. III - 3). Supondremos que $q(x)$ y $p(x)$ son primos entre sí (Cap. III - 4). El gráfico de esta función racional tiene entonces intersección con el eje x en las raíces reales de $q(x)$ y asíntotas verticales correspondientes a las raíces reales de $p(x)$. Las asíntotas horizontales pueden igualmente obtenerse de inmediato (Ejercicios 2 y 3). Sea

$$q(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad a_0 \neq 0,$$
$$p(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m, \quad b_0 \neq 0.$$

Si $n < m$, el gráfico de $q(x)/p(x)$ tiene como asíntota al eje x en ambos sentidos, positivo y negativo. Si $n = m$, el gráfico tiene a la recta $y = a_0/b_0$ como asíntota horizontal en ambos sentidos. Si $n > m$, no hay asíntotas horizontales. Frecuentemente se obtienen otras asíntotas de funciones racionales. (Ejercicio 5). Gracias a estas pocas reglas y a que la función cambia de signo en una asíntota vertical $x = b$ si y sólo si la raíz $x = b$ es de multiplicidad impar en $p(x)$, no es más difícil hacer el gráfico de la función racional $y = q(x)/p(x)$ que el del polinomio $z = p(x) \cdot q(x)$. En realidad, y y z tienen el mismo signo siempre que $z \neq 0$, dado que $z = y\,[p(x)]^2$.

Consideremos el ejemplo

$$y = \frac{(x-2)(x^2-4)(2x-7)}{x(x-1)^2(x+3)}.$$

La curva tiene intersecciones con el eje x en 2, 2, -2, y $\frac{7}{2}$, asíntotas verticales en $x = 0$, 1, 1, -3, y asíntota horizontal $y = 2$. En la Fig. VII - 12 se presenta el aspecto general del gráfico. Se puede lograr un gráfico más exacto por medio del cálculo para ob-

tener los puntos de inflexión o simplemente trazando unos cuantos puntos más.

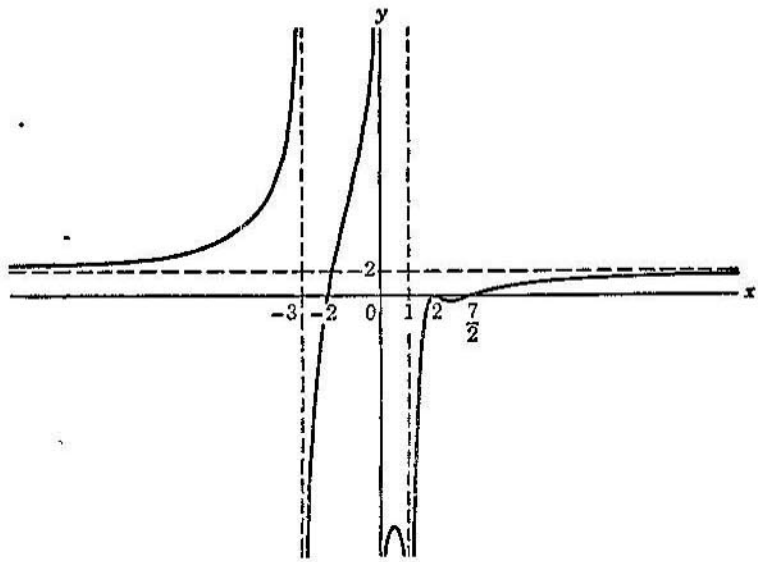


FIG. VII-12

Este método puede emplearse también para hacer el gráfico de funciones de la forma $p(x)t^n = q(x)$. Considérese primero $p(x)y = q(x)$ y luego hágase $t = \pm\sqrt{y}$. El gráfico en t y x será real solamente para aquellos valores de x correspondientes a valores nulos o positivos de y. Por ejemplo, para trazar el gráfico de la función

$$f(x, t) = x(x - 1)^2(x + 3)t^2 - (x - 2)(x^2 - 4)(2x - 7) = 0,$$

hacemos primero el gráfico de la ecuación correspondiente, en que $y = t^2$, como en el ejemplo anterior. Del gráfico anterior resulta evidente que el gráfico de $f(x, t)$ es real solamente para valores de x en los intervalos $x < -3$, $-2 \leqq x < 0$, $x = 2$, y $7/2 \leqq x$. Luego el punto (2,0) es un punto aislado, la recta $x = -3$ es una asíntota vertical, las rectas $t = \pm\sqrt{2}$ son asíntotas horizontales, y el gráfico de $f(x, t)$ es de la forma que se muestra en la Fig. VII - 13.

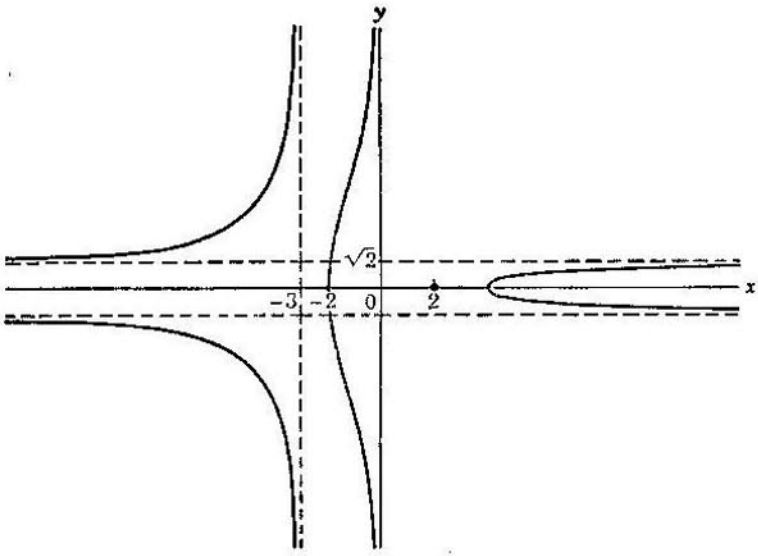


FIG. VII-13

EJERCICIOS:

1. Determinar las intersecciones de las curvas siguientes con los ejes x e y:

(a) $x/a + y/b = 1$,
(b) $y = x^2 - 2x$,
(c) $(x^2 - 4)y = x + 5$,
(d) $x^2y - 2xy - x^2 + x + 6 = 0$,
(e) $(x^2 - 2x - 3)y = x^3 - 2x^2 + x$,
(f) $(x + 1)y^2 = x(x - 2)^2(x - 3)$.

2. Considérese $y = q(x)/p(x)$ en la forma $yp(x) = q(x)$ y examínense las asíntotas horizontales y verticales, valiéndose de los coeficientes de las potencias de mayor grado de las variables.

3. La asíntota horizontal de $y = q(x)/p(x)$ puede determinarse como $y = \lim_{x\to\infty} q(x)/p(x)$ siempre que el límite (finito) exista. Valerse de los métodos del Cap. III-11 para verificar que los enunciados formulados respecto de las asíntotas horizontales en el Ejercicio 2, son válidos también según esta nueva definición.

4. Obtener las asíntotas verticales y horizontales de las curvas del Ejercicio 1, toda vez que existan.

5. Escribir $y = q(x)/p(x)$ en la forma $s(x)/p(x) + r(x)$ en donde el grado de $s(x)$ sea menor que el de $p(x)$ y demostrar que el gráfico de la función racional dada es asintótico con el gráfico del polinomio $y = r(x)$.

VII-7 FUNCIONES ALGEBRAICAS. Una ecuación polinomia $f(x, y) = 0$, en que $f(x,y)$ se considera como un polinomio en y con coeficientes pertenecientes al anillo de los polinomios en x con coeficientes complejos, determina a y como una función algebraica (Cap. III - 16) y tiene como gráfico real una *curva plana algebraica*. El concepto de función algebraica es una ampliación del concepto de polinomio porque todo polinomio $p(x)$ satisface $f(x,y) = y - p(x)$, es decir, un polinomio es un caso especial de una función algebraica que surge cuando $f(x,y)$ tiene la forma $y - p(x)$. Análogamente, una función racional (Cap. VII - 6) es un caso especial de una función algebraica que se origina cuando $f(x,y)$ tiene la forma $p(x)y - q(x)$.

Hemos visto (Cap. III - 10) que cualquier polinomio $p(x)$ es una función uniforme de x. Además, una función racional de x es uniforme siempre que esté definida (Cap. III - 3). Sin embargo, una función algebraica definida por una ecuación polinomia $f(x,y) = 0$ de grado n en y, puede tener n valores de y que corresponden a un valor dado de x. Por ejemplo, $y^2 - x = 0$ tiene asociados dos valores reales de y con cada valor positivo de x. En esta sección nuestro estudio se limitará a una introducción muy breve de una representación gráfica (la superficie de Riemann) de los n valores de la función algebraica y (no necesariamente reales y distintos), que corresponden a cada valor de x (Teorema IV - 2).

A menudo nos hemos referido a un polinomio con coeficientes reales con el nombre de un "polinomio real". En algunos textos se dice que una *curva* es real si la función $f(x,y)$ tiene coeficientes reales. Según esta definición una curva real puede tener sólo puntos imaginarios, como en el caso de $x^2 + y^2 + 1$. Nosotros denominaremos un *gráfico real* de cualquier curva a aquél compuesto de los puntos reales cuyas coordenadas (n-tuplos reales) hacen que la función se anule.

En el Capítulo I, al estudiar nuestro sistema de números, ampliamos el sistema de números racionales y obtuvimos el sistema de números reales con el objeto de conseguir un sistema continuo (sin interrupciones en el eje de los números reales). En seguida ampliamos el sistema de los números reales y obtuvimos el sistema de los números complejos y examinamos la propiedad de todo polinomio de grado n en una sola variable con coeficientes complejos que ten-

gan exactamente n raíces complejas (Teorema IV - 2). Esto significa que el sistema de números complejos es cerrado algebraicamente.

Se puede expresar geométricamente esto mismo en forma análoga, como sigue: se consideró una recta de puntos racionales con el objeto de obtener las raíces de todas las ecuaciones lineales con coeficientes enteros o racionales. Esta recta se amplió para obtener la recta real y asegurarse la continuidad, a saber, que cualquiera curva que una dos puntos situados a los "lados opuestos" de una recta, corte a la recta. Finalmente, la recta real se amplió y se obtuvo el plano complejo con el objeto de representar todas las raíces de cualquier polinomio en una variable con coeficientes complejos.

Geométricamente, se puede hacer una ampliación análoga respecto de los gráficos de las funciones algebraicas. En un espacio de dos coordenadas complejas, la ecuación $y^2 - x = 0$ asocia exactamente dos valores de y con cada valor complejo de x. Estos valores de y son reales y distintos si x es positivo, reales e iguales si $x = 0$, conjugados imaginarios si x es negativo. Es difícil formarse una imagen de este espacio, ya que corresponde a un espacio euclidiano tetradimensional. La variable compleja x está definida esencialmente sobre un plano euclidiano. Los dos valores de y pueden identificarse con dos superficies u hojas $y = +\sqrt{x}$ e $y = -\sqrt{x}$. En esta nueva superficie de dos hojas, denominada la *superficie de Riemann* de la función $y^2 - x = 0$, la función algebraica $y = f(x)$ es uniforme. Las hojas de una superficie de Riemann suelen cruzarse en puntos (denominados puntos de ramificación), ya que en un espacio de cuatro dimensiones, dos planos pueden cortarse en un solo punto. Aun cuando esta propiedad dificulta la formación de una imagen mental al respecto, el concepto de hojas ha resultado ser muy útil.

En general, se asocia con toda función algebraica $y(x)$, definida por una ecuación polinomia $f(x, y) = 0$ de grado n en y, una superficie de Riemann de n hojas en la cual la función es uniforme. La superficie de Riemann es esencialmente el gráfico de la función en un espacio con dos coordenadas complejas. Se pueden estudiar los puntos de la superficie de Riemann en la proximidad a los puntos correspondientes a $x = a$ por medio de desarrollos de series infinitas (Cap. III-11) en una variable t, en que $x = a + t^r$ (Bibliografía Nº 8; pág. 32). Un estudio cabal de este

más bien complicado procedimiento puede consultarse en (Bibliografía Nº 8).

El resto de este capítulo está dedicado a unos cuantos procedimientos prácticos para la construcción de gráficos reales, a la resolución gráfica de ecuaciones algebraicas y a la determinación de ecuaciones empíricas.

EJERCICIOS:

1. Dar tres ejemplos de cada uno de los siguientes tipos de funciones algebraicas de x: a) función polinomia; b) función racional que no sea un polinomio; c) función algebraica, pero que no sea función racional.
2. Indicar el número de hojas en la superficie de Riemann de cada una de las funciones escritas en el Ejercicio 1.

VII-8 TRAZADO DE CURVAS. El trazado de la curva de una ecuación dada puede efectuarse construyendo la curva mecánicamente, trazando numerosos puntos con cierto grado de precisión o trazando unos pocos puntos seleccionados y determinando la forma de la curva de acuerdo con su simetría, sus puntos singulares y sus asíntotas. Consideraremos brevemente cada uno de estos métodos.

Alfred Bray Kempe resolvió completamente, en teoría, el problema de construir mecánicamente el gráfico real de cualquiera curva plana algebraica $f(x, y) = 0$ de grado n empleando polígonos articulados (Cap. VI-9). En la práctica, estos mecanismos suelen complicarse mucho y hacerse engorrosos a medida que n aumenta. Sin embargo, pueden construirse convenientemente muchas curvas planas corrientes utilizando polígonos articulados. Yates (Bibliografía Nº 54) señala la construcción mecánica de muchas curvas, incluso la cardiode, la cassiniana, la cisoide, las secciones cónicas, la lemniscata de Bernoulli y el caracol de Pascal. Todos empleamos compás para trazar un círculo y, posiblemente, una cuerda enlazada a espigas fijas en los focos para dibujar una elipse. Algunas personas consideran que un pantógrafo (Ejercicio 4, Cap. VI-9) y algunos otros aparatos mecánicos son muy útiles. No obstante, la mayor parte de los métodos mecánicos requiere demasiado equipo y a menudo aparatos muy especiales, para el uso corriente.

El trazado de una curva de grado n por medio de un gran número de puntos puede ser difícil así como tedioso. Las dificultades que se presentan se deben, algebraicamente, a que las raíces de las ecuaciones polinomias de grado n deben aproximarse; y, geométricamente, a que la sucesión de puntos sobre la curva o la asociación de los puntos trazados no es obvia de inmediato. En general, el método de trazar simplemente puntos es más útil en las curvas unicursales (Cap. VII-5).

Existen varios métodos para simplificar el procedimiento de trazar numerosos puntos del gráfico de una curva cuya ecuación $f(x, y) = 0$ es dada. En primer lugar, es fácil trazar los puntos de intersección de la curva con los ejes coordenados y por lo menos corrientemente son tan fáciles de obtener como cualquier otro: las intersecciones con el eje x son los ceros reales de $f(x, 0)$ y las intersecciones con el eje y son los ceros reales de $f(0, y)$. Por ejemplo, $x^4 + y^4 - 5x + y - 6$ tiene $f(x, 0) = x^4 - 5x - 6$, de donde las intersecciones con el eje x son 6 y -1; $f(0, y) = y^3 + y - 6$, de donde las intersecciones con el eje y son 2 y -3.

En segundo lugar, la curva puede ser simétrica respecto de ciertos ejes o puntos, de modo que sólo una parte del gráfico necesita un trazado cuidadoso y el resto puede obtenerse por simetría. Por ejemplo, el gráfico de $y = x^2$ es simétrico respecto del eje y. En general, el gráfico de $f(x, y)$ es simétrico:

al eje x si $f(x, y) = f(x, -y)$,
al eje y si $f(x, y) = f(-x, y)$,
al origen si $f(x, y) = f(-x, -y)$,
y a la recta $y = x$ si $f(x, y) = f(y, x)$.

Se pueden desarrollar pruebas para determinar la simetría respecto de muchos otros ejes y centros (Ejercicio 3), pero las anteriores son las más comunes y las más fáciles de aplicar (Ejercicio 2).

Otro concepto que simplifica el trazado de puntos es el de las regiones excluidas. Frecuentemente, existen conjuntos de valores de una variable para los cuales el gráfico no tiene ningún valor real. Tales conjuntos de valores se denominan *regiones excluidas*. Por ejemplo, el gráfico de $y = x^2$ no tiene ningún punto real para los valores negativos de y; el gráfico de $y^2 = 2x - x^2$ no tiene ningún punto real cuando $x < 0$ ó $2 < x$; el gráfico de la Fig. VII-13

no tiene ningún punto real cuando $-3 \leqq x < -2$, $0 \leqq x < 2$, ó $2 < x < \frac{7}{2}$.

Frecuentemente, es de especial interés el comportamiento de un gráfico en las proximidades del origen o de algún otro punto. Mediante una traslación $x' = x - a$, $y' = y - b$ el comportamiento de cualquier punto (a, b) puede ser estudiado como el comportamiento respecto del nuevo origen. En general, los términos de menor grado determinan el comportamiento de la curva en las proximidades del origen. Dado cualquier polinomio $f(x, y)$, sea $g(x, y) = 0$ la ecuación polinomia que resulta igualando a cero los términos de menor grado de $f(x, y)$. Si $g(x, y)$ es constante y diferente de cero, el gráfico de $f(x, y)$ no pasa por el origen. En todo caso, los términos de $g(x, y)$ son del mismo grado, es decir $g(x, y)$ es un *polimonio homogéneo*. Un polimonio homogéneo de grado r en x e y con coeficientes complejos se puede expresar siempre, teóricamente, como el producto de r polimonios lineales con coeficientes complejos. Los gráficos de los factores lineales de $g(x, y)$ son las tangentes a la curva $f(x, y) = 0$ en el origen. Por ejemplo, si $f(x, y) = x^3 + y^3 - 3axy$, en que $a \neq 0$ (Fig. VII-6), entonces $g(x, y) = -3axy$ y las tangentes en el origen son $x = 0$ e $y = 0$. Análogamente, el gráfico de $x^3 + xy^2 + ax^2 - ay^2 = 0$ tiene tangentes $x + y = 0$ y $x - y = 0$ en el origen.

Para hacer el gráfico de las funciones racionales (Cap. VII-6), son muy útiles las asíntotas horizontales y verticales. En general, dado cualquier polinomio $f(x, y)$ de grado n, los términos de grado n y $n - 1$ determinan el comportamiento de la curva en los valores numéricos grandes de las coordenadas. Sea $h(x, y)$ el polinomio homogéneo compuesto por los términos de grado n de $f(x, y)$. Los gráficos reales de los factores lineales de $h(x, y)$ son paralelos a las asíntotas del gráfico de $f(x, y)$. En el ejemplo $f(x, y) = x^3 + y^3 - 3axy$ (Fig. VII-6), $h(x, y) = x^3 + y^3$, y la única asíntota es paralela a $x + y = 0$. En general las ecuaciones de las asíntotas dependen de los términos de grados n y $n - 1$ (Bibliografía Nº 27, pág. 13). Si $h(x, y)$ no contiene un término x^n, sea $p(y)$ el coeficiente de la potencia mayor de x en el polinomio original $f(x, y)$. Entonces los gráficos de los factores lineales de $p(y)$ son las asíntotas horizontales de $f(x, y)$. Lo mismo se puede decir respecto de las asíntotas verticales, como se ilustró en el Cap. VII-6 al considerar las funciones racionales en la forma $p(x)y - q(x)$. La teoría

general de las asíntotas incluye el Diagrama de Newton o triángulo analítico (Bibliografía Nº 27, pág. 15).

Hasta aquí hemos estudiado el uso de las intersecciones con los ejes coordenados, de la simetría, de las regiones excluidas, de las tangentes en el origen (o en cualquier otro punto determinado), y de las asíntotas en el trazado del gráfico de un polinomio $f(x, y)$. Los puntos singulares (Cap. VII-5) pueden usarse también en forma efectiva. Frost (Bibliografía Nº 22) y Johnson (Bibliografía Nº 27) tratan este tema en forma elemental y no suponen conocimiento alguno de cálculo. Hilton (Bibliografía Nº 26) aprovecha efizcamente conceptos matemáticos más avanzados. Concluiremos esta sección con un solo ejemplo de los eficaces métodos empleados en textos más avanzados, tales como (Bibliografía Nº 26).

Dado cualquier polinomio $f(x, y)$ de grado n, podemos hacer que cada término del polinomio sea de grado n insertando una potencia adecuada de z y obtener, de este modo, un polinomio homogéneo $f(x, y, z)$. Por ejemplo, si $f(x, y) = x^3 + y^3 - 3xy$, entonces $f(x, y, z) = x^3 + y^3 - 3xyz$. En seguida, empleamos la notación f_x para indicar la primera derivada parcial respecto de x de $f(x, y, z)$, es decir, la primera derivada de $f(x, y, z)$ con respecto de x, en que y y z se consideran constantes. Análogamente, f_{xy} es la derivada parcial de f_x con respecto de y, etc. En el caso de $f(x, y, z) = x^3 + y^3 - 3xyz$, tenemos:

$$\begin{array}{lll} f_x = 3x^2 - 3yz, & f_y = 3y^2 - 3xz, & f_z = -3xy, \\ f_{xx} = 6x, & f_{yy} = 6y, & f_{zz} = 0, \\ f_{xy} = f_{yx} = -3z, & f_{yz} = f_{zy} = -3x; & f_{zx} = f_{xz} = -3y \end{array}$$

El gráfico del determinante de las derivadas parciales de segundo orden de $f(x, y, z)$,

$$H(x, y, z) = \begin{vmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{vmatrix},$$

se denomina *el hessiano* de la curva dada (Bibliografía Nº 26, pág. 98). La importancia del hessiano se debe a que las intersecciones de una curva con su hessiano son precisamente los puntos singulares y los puntos de inflexión de la curva dada. Por ejemplo, el hessiano de $x^3 + y^3 - 3xyz$ es el gráfico del polinomio

$$H(x, y, z) = \begin{vmatrix} 6x & -3z & -3y \\ -3z & 6y & -3x \\ -3y & -3x & 0 \end{vmatrix} = -54(x^3 + y^3).$$

Las intersecciones de los gráficos $f(x, y) = x^3 + y^3 - 3xy$ y $H(x, y) = -54(x^3 + y^3)$ deben también encontrarse sobre $54f(x, y) + H(x, y)$ y, por lo tanto, sobre por lo menos uno de los ejes coordenados. En consecuencia, el único punto singular o punto de inflexión del gráfico de $f(x, y) = x^3 + y^3 - 3xy$ se encuentra en el origen (Fig. VII-6).

En esta sección hemos considerado varios métodos de hacer gráficos de curvas planas. No obstante, de ninguna manera hemos agotado el tema, ya que se puede escribir fácilmente la ecuación de una curva plana de grado superior cuyo gráfico no se puede obtener de inmediato por medio de estos métodos. En consecuencia, al reconocer la dificultad de representar gráficamente la mayoría de las curvas planas de grado superior, consideraremos el presente estudio sólo como un breve tratado de los métodos que pueden facilitar la representación gráfica de cualquiera curva plana dada de grado superior, pero no se puede esperar convertir la representación gráfica en una simple rutina. En la sección que sigue estudiaremos unos cuantos tipos especiales de gráficos.

EJERCICIOS

1. Encontrar las intersecciones de las siguientes curvas con el eje x, y con el eje y:

a) $x^2 - 8x + y^2 + 7y + 12 = 0$;
b) $x^3 + y^3 - 3axy = 0$ (Fig. VII-6), folio de Descartes;
c) $x^2y^2 + x^2 - y^4 = 0$;
d) $xy^2 - x - 4y = 0$;
e) $x^2y^2 - x^2 - 4y^2 = 0$;
f) $x^2y + a^2y - a^3 = 0$, curva versiera de Agnesi;
g) $x^3 + xy^2 - 2ay^2 = 0$, cisoide de Diocles;
h) $x^3 + xy^2 + ay^2 - 3ax^2 = 0$ (Fig. VI-5), trisectriz;
i) $x^3 + xy^2 + ax^2 - ay^2 = 0$, estrofoide;
j) $x^2y + b^2y - a^2x = 0$, serpentina;
k) $y^2 = x(x - 1)(x - 2)$;
l) $y^2 = -x^2(x + 1)(x - 2)$.

2. Probar la simetría de cada una de las curvas del Ejercicio 1, con respecto a) al eje x; b) al eje y; c) al origen; d) a la recta $x = y$.

3. Inventar demostraciones para probar la simetría con respecto a cada una de las siguientes rectas: a) $x = 1$; b) $x = a$; c) $y = b$; d) $x - y = 0$.

4. Indicar las regiones excluídas, si existe alguna, respecto de x e y en los gráficos de cada una de las curvas del Ejercicio 1.

5. Encontrar las tangentes en el origen de las curvas siguientes:

(a) $xy^2 = x^3$, (c) $(x + 2)y^2 = x^2(x + 1)$,
(b) $y^2 = x^2(x - 1)$, (d) $xy^2 - x^3 = x^4$.

6. Hallar las tangentes en el origen, si existe alguna, de los gráficos de cada una de las curvas del Ejercicio 1.

7. Discutir el comportamiento de $x^3 + y^3 - 6xy$ en (3,3).

8. Hallar los puntos singulares de cada una de las curvas siguientes empleando el hessiano: a) $x^2 - xy^2 - y^4$; b) $x^3 + xy^2 - x$.

9. Hacer el gráfico de las curvas del Ejercicio 8. [*Indicación:* la curva del Ejercicio 8 (b) es reducible (Cap. VII-9)].

VII-9 GRAFICOS ESPECIALES. Ahora vamos a estudiar cuatro métodos especiales para hacer gráficos. Estudiaremos los gráficos de curvas reducibles, gráficos que resultan de la composición de ordenadas, gráficos de funciones trascendentes y curva de Peano (curva que llena un área).

Todas las veces que el polinomio $f(x, y)$ puede factorizarse como

$$f(x, y) = g(x, y) \cdot h(x, y),$$

se dice que el gráfico de $f(x, y)$ es *reducible* y comprende a la totalidad de los puntos sobre los gráficos de $g(x, y)$ y $h(x, y)$. Los gráficos de los factores de $f(x, y)$ se denominan *componentes* del gráfico de $f(x, y)$. Por ejemplo, el gráfico de $x^3 + xy^2 - x$ (Ejercicio 8 b), Cap. VII-8) tiene dos componentes correspondientes a los factores x y $x^2 + y^2 - 1$, respectivamente. De esta manera puede obtenerse el gráfico de cualquier curva reducible haciendo el gráfico de cada uno de sus componentes.

La representación gráfica de $f(x, y)$ suele simplificarse a menudo resolviendo la función para una de las variables, como ser, $y = r(x)$, en que $r(x)$ no es necesariamente un polinomio. Por ejemplo,

$$2x^2 + y^2 - 2xy + 2x - 2,$$

al resolverla respecto de y, resulta:

$$y = x \pm \sqrt{2 - 2x - x^2},$$

que se puede representar gráficamente como $y = y_1 + y_2$, en donde $y_1 = x$, y

$$y_2 = \pm \sqrt{2 - 2x - x^2}$$

ó $(x + 1)^2 + y_2^2 = 3$. Si $f(x, y) = 0$ se resuelve respecto de y, este método de trazar la curva se denomina representación gráfica por *composición de ordenadas.*

En nuestro estudio nos hemos preocupado principalmente de los gráficos de polinomios. También pueden determinarse gráficos de funciones trascendentes tales como $y = \text{sen } x$ o $y = \log_p x$, en que $1 < p$, por medio de varios polinomios:

$$\begin{aligned} y &= -x \text{ si } x < 0, \\ &= 5 \text{ si } x = 0, \\ &= x^2 \text{ si } x > 0, \end{aligned}$$

o por otros símbolos tales como $y = |x|$ o $y = [x]$, donde el x entre paréntesis indica el mayor entero menor que o igual a x. Varias funciones semejantes a éstas se tratan en (Bibliografía Nº 24, págs. 55-60). Es posible aún definir y, por muy equívoco que sea su gráfico, debido a la distancia entre las marcas correspondientes a los puntos trazados. Por ejemplo, supongamos

$$\begin{aligned} y &= 1 \text{ si } x \text{ es racional}, \\ &= 0 \text{ si } x \text{ es irracional}. \end{aligned}$$

Dado que los números racionales son densos y los números irracionales son infinitos (Cap. 1-13) en todo segmento (a, b), siendo $a < b$, el gráfico de la función uniforme anterior resulta estar compuesto de dos rectas $y = 0$ e $y = 1$. En el Ejercicio 3, pueden hallarse varios otros ejemplos de gráficos que no pueden darse por un solo polinomio en x y en y.

Concluiremos nuestro estudio sobre el trazado de gráficos refiriéndonos a una curva con propiedades muy excepcionales, el arco de Peano, que llena un área, pues pasa por todos los puntos

interiores de un cuadrado. Se denomina arco porque cada punto de él puede determinarse por un solo valor real del parámetro t, $0 < t < 1$, del mismo modo, que los puntos interiores de un segmento unidad sobre el eje x pueden determinarse por un solo valor real de x, $0 < x < 1$. En (Bibliografía Nº 21, pág. 56) se puede consultar una descripción de la manera en que se asocian los puntos interiores del cuadrado con los valores reales de t, siendo $0 < t < 1$. Este arco tiene importancia en las teorías matemáticas ya que establece una correspondencia biunívoca entre los puntos de un elemento de un área (de dos dimensiones) y los puntos de un segmento de recta (de una dimensión).

EJERCICIOS

1. Trazar los gráficos de:

   (a) $x(x^2 + y^2 - 2x + 2y - 7)$,
   (b) $(x^2 - y^2)(x^2 + y^2 - 1)$,
   (c) $x^3 - x^2y - 2x + 2y$.

2. Representar gráficamente por composición de ordenadas o abscisas:

   (a) $y = x^5 + 1$,
   (b) $x^2 - 4xy + 4y^2 = x - 4$,
   (c) $x^2 + 6xy + 9y^2 + x + 6y + 1 = 0$,
   (d) $y = x + \text{sen } x$.

3. Hacer los gráficos de:

(a) $y = x - [x]$.
(b) $y = |x|$.
(c) $y = -x$ si $x \leqq 0$
    $= x$ si $x > 0$.
(d) $y = \sqrt{x}$ si x es el cuadrado de un entero,
    $= x$ en todos los demás casos
(e) $y = 1$ si x es racional,
    $= -1$ si x es irracional;
(f) $y^2 = |x|$.
(g) $y^2 = x - [x]$.

VII - 10 SOLUCIONES GRAFICAS. Si para obtener la solución de un problema se necesita observar las intersecciones de rectas y curvas sobre un plano, ésta es necesariamente una solución aproximada. No obstante, una solución aproximada

suele ser muy útil. La adición gráfica que sigue es un ejemplo trivial del procedimiento general.

Consideremos la familia F de rectas $x + y = C$ y hagamos un cuadro trazando las rectas correspondientes a valores de C menores en valor absoluto que algún número positivo N. Puede hallarse gráficamente la suma $a + b$ de dos números reales trazando el punto (a, b) y observando el valor particular de C que correspondería a la recta de la familia de rectas F que pasa por (a, b).

Las aplicaciones de los métodos gráficos son muy numerosas. En la Bibliografía Nº 46 se consideran la adición, la sustracción, la multiplicación y división, interés simple y compuesto, resolución de ecuaciones cuadráticas, cúbicas y cuárticas, la integración y la diferenciación. El uso de las curvas en el problema de la trisección se estudió en el Cap. VI-7. Muchas otras aplicaciones de los métodos gráficos pueden consultarse en la Bibliografía Nº 33.

Otra aplicación de las soluciones gráficas se encuentra en las reglas de cálculo y nomogramas. Por ejemplo, en la mayoría de las reglas de cálculo se puede hallar la raíz cuadrada de un número en la escala A mirando directamente debajo de ella (suponiendo que los extremos de las escalas se corresponden) sobre la escala C. La correspondencia entre el número y su raíz cuadrada se puede mirar comúnmente gracias a un hilo cruzado (recta fina y movible perpendicular a las escalas). Por esto, la regla de cálculo es un caso especial de gráfico alineado o nomograma. Muchos nomogramas consisten en tres rectas o curvas situadas con precisión, con escalas (posiblemente muy diferentes en unidades y en significado) marcadas sobre cada una de ellas. El nomograma se usa entonces colocando una reglita sobre puntos en dos de las escalas, según los datos dados, y leyendo el resultado en la tercera escala. Maurice d'Ocagne inventó algunos excelentes nomogramas y desarrolló métodos para resolver ecuaciones en más de dos variables en el plano. Muchos de los procedimientos publicados en libros más recientes se basan sobre el trabajo de d'Ocagne. Para pormenores respecto de la construcción y uso de nomogramas se remite al lector a textos especiales sobre la materia. Concluiremos nuestro estudio de las representaciones gráficas con una breve discusión del problema de hallar una ecuación o curva que corresponda a un conjunto dado de puntos.

EJERCICIOS

1. Dibujar gráficos que puedan servir para aproximar cada uno de los siguientes, siendo $0 \leqq b \leqq 10$:

(a) $\sqrt{b}$, (c) $\sqrt[3]{b}$, (e) $\sqrt{b+3}$,
(b) $b^2 + 1$, (d) $b^{\frac{1}{3}}$, (f) $\sqrt{b} + 3$.

2. Dibujar varias curvas de una familia de curvas que sirvan para aproximar cada una de las siguientes:

(a) $a + b$, (c) ab, (e) $a^2 + 2ab + b^2$.
(b) $a - b$, (d) a/b,

3. Resolver gráficamente los siguientes sistemas de ecuaciones y desigualdades:

(a) $y = x$,
$y < x^2$,
$y^2 > x$.

(b) $1 - y^2 > x^2$,
$0 < x < y$.

(c) $\sin x < y \leqq 1$,
$|x| < 3$.

(d) $1/x > 1/y$,
$x^2 + y^2 = 25$.

VII-11 DETERMINACION DE CURVAS.

Hasta aquí hemos trazado curvas de ecuaciones dadas. En esta sección, supondremos que se da un conjunto de valores correspondientes a dos variables y procuraremos encontrar la ecuación entre las dos variables que mejor convenga a los datos dados y a las condiciones del problema. A menudo los datos se han obtenido por medio de la observación o de la experimentación y al formar una ecuación entre las variables se puede lograr una mejor comprensión del problema.

Siempre es posible hallar una curva de grado menor o igual a $n - 1$ que pase por n puntos dados. Sin embargo, puede ocurrir que nuevos conjuntos de valores del gráfico no se aproximen a los nuevos valores correspondientes del problema. Nos referiremos a algunos métodos para determinar una ecuación, denominada *ecuación empírica,* que se satisfaga aproximadamente con los datos dados. Por ser la línea recta la curva cuya imagen se capta más fácilmente, la consideraremos en varios tipos de escalas coordenadas. Para medir si una ecuación empírica es adecuada o no se suele

utilizar promedios o el método de los cuadrados menores, es decir, se reduce al mínimo la suma de los cuadrados de las diferencias entre los resultados de los datos dados y aquellos que se desprenden de la ecuación. El tema de la determinación de curvas a partir de datos dados entre las variables se estudia en muchos textos de geometría analítica, por ejemplo, en (Bibliografía Nº 38, págs. 204-223). Se pueden consultar estudios más completos sobre esta materia en Bibliogría Nº 14, págs. 3-88; Nº 33, págs. 120-169.

El gráfico de $y = ax + b$ en papel corriente para gráficos es una línea recta con pendiente a y que corta al eje y en b. A la inversa, cada vez que los puntos correspondientes a los datos dados parecen encontrarse sobre una línea recta en papel corriente para gráficos, ellos pueden satisfacer (mediante un cambio de coordenadas si la recta es paralela al eje y) muy aproximadamente una ecuación de la forma $y = ax + b$. Las constantes a y b pueden calcularse fácilmente basándose sobre los datos dados o en el gráfico de la recta.

El método de los promedios se aplica a la relación lineal $y = ax + b$, como sigue: Por ejemplo, los pares dados de valores

x	1	2	3	4	5	6	7
y	3.20	4.30	4.80	6.10	7.00	8.20	9.10

se dividen en dos conjuntos (dado que hay que determinar dos constantes) aproximadamente iguales en número. Por ejemplo, tomemos los primeros tres y los últimos cuatro pares de datos anteriores. En la relación lineal se sustituyen los pares de cada conjunto y obtenemos las *ecuaciones aproximadas*

$$\begin{aligned} 3.2 &= a + b, & 6.1 &= 4a + b, \\ 4.3 &= 2a + b, & 7.0 &= 5a + b, \\ 4.8 &= 3a + b, & 8.2 &= 6a + b, \\ & & 9.1 &= 7a + b; \end{aligned}$$

Los elementos de cada conjunto se suman

$$12.3 = 6a + 3b, \quad 30.4 = 22a + 4b,$$

y las dos ecuaciones que resultan se resuelven simultáneamente para $a = 1$ y $b = 2.1$ para obtener la ecuación empírica $y = x + 2.1$. También puede usarse el método de los promedios para adecuar una parábola $y = ax^2 + bx + c$ a partir de los datos dividiendo los pares de valores en tres conjuntos y resolviendo las

tres ecuaciones lineales resultantes respecto de tres parámetros a, b, c.

Cuando se aplica el método de los cuadrados menores a la ecuación lineal $y = ax + b$ determina principalmente valores de a y b tales que

$$D = \sum_{j=1}^{n} (ax_j + b - y_j)^2$$

es un mínimo donde hay n pares de valores (x_j, y_j), $j = 1, 2, \ldots, n$, en los datos dados. Esto se puede hacer resolviendo las dos ecuaciones lineales diferenciales $\delta D/\delta a = 0$, $\delta D/\delta b = 0$ simultáneamente para a y b. También se puede hacer (Bibliografía Nº 38; págs. 219-222) resolviendo simultáneamente las ecuaciones

$$\sum y_j = a \sum x_j + nb,$$
$$\sum x_j y_j = a \sum x_j^2 + b \sum x_j.$$

Si las ecuaciones aproximadas $y_j = ax_j + b$ forman una columna y las $x_j y_j = ax_j^2 + bx_j$ otra, resulta para el ejemplo anterior

3.2 =	a +	b	3.2 =	a +	b
4.3 =	$2a$ +	b	8.6 =	$4a$ +	$2b$
4.8 =	$3a$ +	b	14.4 =	$9a$ +	$3b$
6.1 =	$4a$ +	b	24.4 =	$16a$ +	$4b$
7. =	$5a$ +	b	35. =	$25a$ +	$5b$
8.2 =	$6a$ +	b	49.2 =	$36a$ +	$6b$
9.1 =	$7a$ +	b	63.7 =	$49a$ +	$7b$
42.7 =	$28a$ +	$7b$	198.5 =	$140a$ +	$28b$

de donde $a = 0.99$ y $b = 2.14$, y resulta la ecuación empírica $y = 0.99x + 2.14$. Es obvio, que estos métodos se pueden aplicar con ligeras modificaciones a las relaciones lineales $\log y = a \log x + \log b$ y $\log y = ax + b$, la que acabamos de considerar.

La ecuación $y = bx^a$ es equivalente a $\log y = a \log x + \log b$ que es lineal en $\log y$ y en $\log x$. En consecuencia, se emplea papel logarítmico, donde las distancias Ox y Oy representan los logaritmos de x y de y respectivamente, en vez de sus magnitudes. Siempre que los puntos correspondeintes a los datos dados se presenten sobre una línea recta en el papel logarítmico, ellos pueden satisfacer aproximadamente una ecuación de la forma $y = bx^a$

y las constantes pueden determinarse fácilmente por medio del gráfico. Este método se puede hacer extensivo a $y = bx^a + c$ considerándola en la forma $\log (y - c) = a \log x + \log b$. El valor de c puede calcularse por ensayo y error o gráficamente (Bibliografía Nº 14; pág. 12).

Hacemos notar también que $y = 10^{bx^a} + c$ puede considerarse en la forma $\log (y - c) = ax + b$ como un gráfico lineal en papel semilogarítmico. Finalmente, cuando la razón de cambio de una variable con respecto a la otra es lineal, tenemos

$$\frac{\Delta y}{\Delta x} = 2ax + b$$

y las variables pueden relacionarse por medio de

$$\frac{dy}{dx} = 2ax + b \quad \text{or} \quad y = ax^2 + bx + c.$$

Si los recíprocos de x e y están relacionados linealmente, es decir,

$$\frac{1}{y} = \frac{b}{x} + a,$$

entonces

$$y = \frac{x}{ax + b}.$$

Hay otros tipos comunes de ecuaciones empíricas, pero las anteriores dan a conocer uno de los usos de los diferentes papeles coordenados y algunas de las ventajas de los métodos gráficos. Un estudio más amplio de las ecuaciones empíricas puede consultarse en (Bibliografía Nº 14) y en muchos textos sobre estadística.

EJERCICIOS

1. Por medio del método de los promedios hallar una ecuación de la forma $y = ax + b$ que se satisfaga aproximadamente con los siguientes datos:

x	1	2	3	5	10	12
y	2.2	4.3	6.5	11	21	24

2. Trazar los puntos dados sobre la recta que se obtuvo en el Ejercicio 1.

3. Hallar una ecuación de la forma $y = ax^2 + bx + c$ para los datos dados en el Ejercicio 1.

VII - 12 C O N C L U S I O N . En este capítulo hemos considerado las relaciones entre los gráficos y las ecuaciones. Desde la Sección 1 hasta la Sección 10 nuestro interés principal residió en obtener el gráfico de una función dada; en la Sección 11 nos preocupamos de hallar una ecuación de cierto tipo valiéndonos de la curva que mejor se ajustara en los puntos ocrrespondientes a ciertos datos dados. Estas consideraciones ilustran la importancia de las relaciones entre los conceptos fundamentales de álgebra y los conceptos fundamentales de geometría. En particular, hemos visto que muchos problemas algebraicos pueden expresarse geométricamente y, análogamente, muchos problemas geométricos (por ejemplo, las construcciones clásicas del Cap. VI) pueden expresarse algebraicamente. Como se puede ver, un estudio de los conceptos básicos de cualquiera rama de las matemáticas, y en particular nuestro estudio de los conceptos fundamentales de álgebra, en este texto, amplían nuestro conocimiento de todos los aspectos de las matemáticas.

Bibliografía

1. ALBERT, A. A., *College Algebra*. New York: McGraw-Hill, 1946.
2. ARCHIBALD, R. C. "Outline of the History of Mathematics", 6ª ed., *American Mathematical Monthly, 56*, Part II, 1949.
3. BALL, W. W. R., *Mathematical Recreations and Essays*. 11ª ed., revisada por H. S. M. Coxeter. New York: Macmillan, 1939.
4. BERGER, E. J. "Devices for a Mathematical Laboratory", *The Mathematics Teacher, 44*, 34, 1951.
5. BERGER, E. J., "Devices for a Mathematical Laboratory", *The Mathematics Teacher, 45*, 287, 1952.
6. BIRKHOFF, G. D. and BEATLEY, R., *Basic Geometry*. Chicago: Scott, Foresman and Co., 1940.
7. BIRKHOFF, G. and MACLANE, S., *A Survey of Modern Algebra*. New York: Macmillan, 1941.
8. BLISS, G. A., *Algebraic Functions*. Colloquium Publications, Vol. 16. New York: American Mathematical Society, 1933.
9. BÔCHER, MAXIME, *Introduction to Higher Algebra*. New York: Macmillan, 1907.
10. BOURBAKI, NICHOLAS, "The Architecture of Mathematics", *American Mathematical Monthly, 57*, 221-232, 1950.
11. COOLIDGE, J. L., *A History of the Conic Sections and Quadric Surfaces*. Oxford: Clarendon Press, 1945.
12. COURANT, R., *Differential and Integral Calculus*. Vol. I. E. J. McShane, traductor. New York: Nordemann Publishing Co., Inc., 1938.
13. COURANT, R. and ROBBINS, H., *What is Mathematics?* New York: Oxford University Press, 1941.
14. DAVIS, D. S., *Empirical Equations and Nomography*. New York: McGraw-Hill, 1943.
15. DICKSON, L. E., "Constructions with Ruler and Compasses", *Monographs on Topics of Modern Mathematics*. J. W. A. Young, Editor. New York: Longmans, Green and Co., 1911, pp. 351-386.
16. DRESDEN, ARNOLD, *Solid Analytical Geometry and Determinants*. New York: Wiley, 1930.
17. DUBISCH, ROY, *The Nature of Number*. New York: Ronald Press, 1952.

18. EISENHART, L. P., *Coordinate Geometry*. Boston: Ginn, 1939.
19. FINE, H. B., *College Algebra*. Boston: Ginn, 1904.
20. FOURREY, E., *Procédés Originaux de Constructions Géométriques*. Paris: Libraire Vuibert, 1924.
21. FRANKLIN, PHILIP, *A Treatise on Advanced Calculus*. New York: Wiley, 1940.
22. FROST, PERCIVAL, *An Elementary Treatise on Curve Tracing*. 2ª ed. London: Macmillan, 1911.
23. GANGULI, SURENDRAMOHAN, *Lectures on the Theory of Plane Curves*. Parts I and II. Calcutta: University of Calcutta, 1919.
24. HARDY, G H., *A Course of Pure Mathematics*. 9ª ed. Cambridge: University Press, 1945.
25. HILSENRATH, JOSEPH, "Linkages", *The Mathematics Teacher, 30*, 277-284, 1937
26. HILTON, HAROLD, *Plane Algebraic Curves*. 2ª ed. London: Oxford University Press, 1932.
27. JOHNSON, W. W., *Curve Tracing in Cartesian Coordinates*. New York, Wiley, 1884.
28. KAMKE, E., *Theory of Sets*. F. Bagemihl, traductor. New York: Dover, 1950.
29. KASNER, E. and NEWMAN, J., *Mathematics and the Imagination*. New York: Simon and Schuster, 1940.
30. KLEIN, FELIX, *Famous Problems of Elementary Geometry*. W. W. Beman and D. E. Smith, traductores. Boston: Ginn, 1897.
31. LANDAU, EDMUND, *Foundations of Analysis*. F. Steinhardt, traductor. New York: Chelsea, 1951.
32. LIEBER, L. R. and LIEBER, H. G., *Galois and the Theory of Groups*. Lancaster, Pa.: Science Press, 1932.
33. LIPKA, JOSEPH, *Graphical and Mechanical Computations*. New York: Wiley, 1918.
34. MCCOY, NEAL H., *Rings and Ideals*. Carus Mathematical Monograph, Nº 8. Buffalo, N. Y.: Mathematical Association of America, 1948.
35. MESERVE, B. E., *Fundamental Concepts of Geometry*. Cambridge, Mass.: Addison-Wesley, 1953.
36. MESERVE, B. E., "Linkages as Visual Aids", *The Mathematics Teacher, 39*, 372-379, 1946.
37. MESERVE, B. E., "The Euclidean Division Algorithm", *Pi Mu Epsilon Journal, 1*, 138-144.
38. MIDDLEMISS, R. R., *Analytic Geometry*. New York: McGraw-Hill, 1945.
39. MUIR, THOMAS, *The Theory of Determinants in the Historical Order of Development*. 4 vols. London: Macmillan, 1906, 1911, 1920, 1923.
40. NAGELL, TRYGVE, *Introduction to Number Theory*. New York: Wiley, 1951.
41. NATIONAL COUNCIL OF TEACHERS OF MATHEMATICS, *Multi-Sensory Aids in the Teaching of Mathematics*. 18th yearbook. New York: Columbia University, 1945.
42. OCAGNE, MAURICE DE, *Traité de Nomographie*. Paris: Gauthier-Villars, 1899.
43. ORE, OYSTEIN, *Number Theory and Its History*. New York: McGraw-Hill, 1948.
44. PERLIS, S., *Theory of Matrices*. Cambridge, Mass.: Addison-Wesley Press, 1952.
45. ROOS, J. D. C. DE, *Linkages: the Different Forms and Uses of Articulated Links*. New York: D. Van Nostrand, 1879.
46. RUNNING, T. R., *Graphical Mathematics*. New York: Wiley, 1927.

47. THOMAS, J. M., *Theory of Equations*. New York: McGraw-Hill, 1938.
48. THOMAS, J. M., "Sturm's Theorem for Multiple Roots", *National Mathematics Magazine, 15*, 391-394, 1941.
49. USPENSKY, J. V., *Theory of Equations*. New York: McGraw-Hill, 1948.
50. USPENSKY, J. V. and HEASLET, M. A., *Elementary Number Theory*. New York: McGraw-Hill, 1939.
51. VANDIVER, H. S., "Fermat's Last Theorem, Its History and the Nature of Known Results Concerning It", *American Mathematical Monthly, 53*, 555-578, 1946.
52. VEBLEN, OSWALD and YOUNG, J. W., *Projective Geometry*. Vol. 2 Boston: Ginn, 1918.
53. WAERDEN, B. L. VAN DER, *Modern Algebra*. Vol. I. Fred Blum, traductor. New York: Ungar, 1949.
54. YATES, R. C., *Curves*. New York: Department of Mathematics, United States Military Academy, 1946.
55. YATES, R. C., *The Trisection Problem*. Baton Rouge. Franklin Press, 1942.

Indice alfabético

A

Abeliano, grupo 61.
Absoluto, valor 39-66.
Absurdo, reducción 42.
Acnodo 328.
Acotación de raíces 206, 210-211.
Adición, propiedades de la 25-26 / según teoría de los conjuntos, 17 / conmutativa 25.
Adjuntar 79-80.
Aislación de raíces 211.
Aleph cero 57.
Algebra, teorema fundamental 184.
Algebraicamente cerrado 73.
Algebraico: ampliación 80 / complemento 253 / curva plana 334 / función 175, 329-336 / número 45.
Algoritmo de la división 88-91, 142-145 / de Euclides 101-106, 148-151.
Analíticas, funciones 176.
Angulo, trisector de 304-308 / de Kempe 307.
Anillo 79 / de enteros 85 / de polinomios 137.
Arábiga, notación 109.
Arco, curva que lo llena 342-343.
Aritmética, teorema fundamental 98.
Aritmético, promedio 37.
Arquímedes, postulado 89, 148 / trisección de ángulos 304.
Asíntotas 330, 338-339 / horizontal 331-332 / vertical 330.
Asociados, polinomios 141.
Axioma de Cantor-Dedekind 52.

B

Base 43, 106-111.
Binarias, operaciones 18-19 / relaciones 19.
Binario, sistema 110-111.
Binomio 136.
Birracional, transformación lineal 193.
Bolzano, teorema 55.
Borel, teorema 55.

C

Cambio de variable 151-153, 181-183.
Campo 61, 79-82 / adjunción a un 80 / ampliación algebraica de un 80-81 / conmutativo 61 / cuociente 80, 139.
Cantor, axioma 52 / teorema 55.
Características 257-258.
Cardan, fórmulas 199.
Cardinales, números 14-20 / transfinito 56.
Cauchy, sucesión 55, 160, 176 / criterio de convergencia 160-161.
Cero 27 / cortadura 48 / deficiencia 329 / divisor 61-62, 86 / de polinomio 178.
Cíclico, grupo 76.
Cilindro 323 / recto 319.
Círculo 318-319 / cuadratura del 300 / punto 318-319.
Chino, teorema chino del resto 130.
Coeficiente 136 / posible 141 / principal 136.
Cofactor 240-241.
Columna, desarrollo de 239 / índice de 223.
Combinación lineal 249.
Complejos, números 63-64, 66 / plano 66.

Complemento algebraico 253-254.
Componente 341.
Composición de ordenadas 342.
Compuesto, número 91.
Común divisor 87, 100, 102, 141, 208.
Común múltiplo 87, 100, 142.
Condicionales, ecuaciones 177
Congruencia 116-130, 153 / lineal 127-130 / módulo, clases 120-123.
Cónica, sección 318-323 / degenerada 319-321.
Conjunto 13 / adición 17 / bien ordenado 31, 89 / cerrado 18-19 / continuo 52 / de coeficientes 141 / denso 35 / elementos de 13 / equivalentes 16 / finitos 15 / infinitos 15-16, 56-60 / numerables 57 / mutuamente excluyentes 17 / no vacío 31 / nulo 17 / numerables infinitos 57 / subconjunto 16-17 / vacío 17, 47.
Conmutativa, adición 25 / grupo 60-61 / multiplicación 28.
Cono recto circular 319.
Construcciones 287-312 / básica 293-295 / clásicas 289-303 / de raíces 296-298 / suposiciones 290.
Constructibles, números 296.
Continuas, fracciones 105-106 / funciones 163-170.
Continuo, número cardinal 60.
Contradictorio 45.
Contrapositivo 42.
Contrario 45.
Convergencia, criterio de Cauchy 160-161.
Convergentes, series 163 / sucesiones 160.
Coordenadas 51-52, 69-70 / intersección 330.
Cortadura 46-50 / abierta 46-47 / cero 48 / cerrada 47 / de Dedekind 46-47.
Correspondencia de uno a uno 14.
Cramer, regla de 222, 260-263.
Criba de Eratóstenes 93.
Cuadrada, matriz 223 / orden de una matriz 236.
Cuadrados menores, método 347.
Cuádricas, superficies 323-327.
Cuadráticas, ecuaciones 196, 319.
Cuadratriz 301.
Cuadratura del círculo 300.
Cuárticas, ecuaciones 200-202.
Cúbica, curva 327-329 / ecuaciones 196-200 / reducida, ecuación 198 / resolvente 201.
Cúbico, paraboloide 328.
Cubo, duplicación del 300.
Cuociente, campo 80 / de números complejos 66-67.
Curva cuártica 329 / cúbica 327-329 / cúbicas cuspidales 329 / cúbicas nodales 329 / determinación de 345-349 / llena un arco 342-343 / plana algebraica 334 / plana de grado superior 327-333 / reducible 341 / trazado de 336-343 / unicursal 329.
Cúspide 328.

D

Decimal, exacto 43 / infinito periódico 43 / infinito no periódico 44 / notación 113-115.
Dedekind, axioma 52 / cortadura 46-47 / postulado 47 / teorema 47.
Deficiencia 329.
Definidas, operaciones 19.
Delos, problema de 300.
De Moivre, teorema 74-79.
Demostración, por eliminación 46 / indirecta 42.
Dependencia lineal 269-270.
Dependiente, variable 154.
Derivada 170-172 / parcial 339 / de polinomios 170-172.
Desarrollo de fila 234-236 / de Laplace 254 / de columna 239.
Descartes, regla de los signos 202-207 / Folio de 328.
Desigualdades (V. Relaciones de orden).
Determinación de curvas 345-349.
Determinante 224 / aplicaciones geométricas 275-286 / de coeficientes sistemas ecuaciones lineales 260-261 / desarrollo de los 245 / desarrollo de columna 238-239 / desarrollo de fila 234-

236 / desarrollo de Laplace 254 / diagonal principal 224 / evaluación 249 / de matriz cuadrada 224 / menores complementario 253 / notación de 223-225 / orden de los 236 / de Vandermonde 251-252.
Diagonal principal de matriz cuadrada 224.
Diagrama de Newton 338-339.
Dígitos 43.
Dilatación 286.
Dimensión de espacios complejos 314 / de espacios euclidianos 313-314.
Diofánticos, problemas 131-133.
Directriz 321.
Discontinuidad 164-167 / evitable 166 / finita 167 / infinita 167 / oscilante 167.
Discriminante 186.
Divergente, serie 163.
Divisibilidad, pruebas 118-120, 179.
División 32 / algoritmo 88-91, 142-145 / sintética 179-182, 206 / sucesión 208.
Divisor 27, 86, 140 / cero 61-62, 86 / común 87 / mayor común 87, 100, 102, 109, 141, 149, 208.
Dobles, puntos 328.
Dominio de una función 155 / de integridad 86.
Duplicación del cubo 300.

E

Ecuaciones, teoría 177-220 / aislar raíces de 211 / aproximadas 345-346 / condicionales 177 / cuadráticas 196, 319 / cuárticas 200-202 / cúbicas 196-200 / cúbicas reducidas 198 / empíricas 345-346 / grado de las 183 / de grado mayor que 186 / que son identidades 177 / número de raíces de 183-185, 202-211 / pitagóricas 131-133 / polinomias 205 / raíces de 177 / raíces múltiples de 212-216 / raíces racionales de 194 / reales 205 / solución de 177, 183, 185-187, 214-220 / transformaciones de raíces de 191-196.
Ecuaciones lineales 260-268 / consistentes, sistema de 262 / determinante de coeficientes 260-261 / homogéneas 260 / matriz ampliada de 264 / teorema fundamental 265.
Elementos, clases de 14 / de un conjunto 13 /de un grupo cíclico 76 / identidad respecto de una operación 27 / inversos 31 / menor de un 240.
Eliminación, demostración por 46.
Elipse 320-322.
Elíptico, paraboloide 324.
Enteros 14, 39 / anillo de 85 / no negativos 29-31, 33 / puntos 51.
Equivalencia, relación de 20-21.
Equivalentes, conjuntos 16.
Eratóstenes, criba de 93.
Espacio complejo 314, 315 / euclidiano 272, 313-314 / tetradimensional 325, 327.
Euclidiano, espacios n-dimensionales 314.
Euclides, algoritmo 101-106, 148-151 / transformaciones 284.
Euler, función ϕ de m 122 / teorema de 126.
Evaluación de determinantes 249.
Excluida, región 337.
Exponencial, notación 27 / representación de los números 69.
Extracción de raíz 32.

F

Factor 27 / teorema del 178.
Factorización única, teorema 98.
Fermat, teorema simple de 126-127 / teorema último de 131-133.
Figura plana 297.
Fila, desarrollo de 234 / índice de 223.
Finitos, números 41.
Foco 321.
Folio de Descartes 328.
Fórmula de Taylor 173 /de Cardan 199.
Fracciones continuas 105-106.
Función 154 / algebraica 175, 329-336 / analítica 175-176 / continua 163-170 / continua, gráfico de las 163 / continua, en un intervalo 166 / continua, en un punto 164 / conti-

tinua, uniformemente 169 / creciente 158 / decreciente 158 / discontinua 164-167 / dominio de una 155 / ϕ de Euler 122-126 / gráfico de una 314-343 / inversa 169 / múltiple 155 / racionales 139, 329-333 / rango de una 155 / uniforme 155 / simétrica 194-196 / de Sturm 208 / trascendente 175-176

G

Geometría, definición de Klein 279.
Geométricas, transformaciones 279-286.
Geométrico, promedio 291, 294.
Grado de las ecuaciones 183 / de un polinomio 136-137.
Gráficas, soluciones 343-345.
Gráfico 313-345 / de una función 163, 314-343 / de polinomios 314-329 / real 334 / simétrico 337 / vacío 314.
Grupo 60-61, 76 / abeliano 61 / cíclico 76 / conmutativo 60-61.

H

Heine-Borel-Lebesgue, teorema 55.
Hessiano 339-340.
Hipérbola 320-322.
Hiperboloide de una hoja 325.
Hiperplano 314.
Homogéneos, polinomios 240, 338
Homotéticas, transformaciones 286.
Horizontal, asíntota 331-332.
Horner, método 218-219.

I

Ideal 153, 154.
Identidad, elementos de 27 / relación de 102, 134 / transformación 285.
Ilimitados, números 53.
Imaginarios, números 64.
Inconmensurable 42.
Independiente, polinomio 142 / variable 154.
Indeterminada 135, 140.
Indicador de m 122.
Indice de columna 223.
Indirecta, demostración 42.
Indo-arábiga, notación 109.
Inducción completa 23 / sistemática 23.
Infinita, discontinuidad 167 / serie 162, 174.
Infinito, conjunto 15-16, 56-60 / decimal 44, 113 / decimal periódico 43 / decimal no periódico 44 / sucesiones 159.
Integridad, dominio de 86.
Interno, producto 255.
Intersección, coordenada 330.
Intervalo 155 / abierto 155 / cerrado 155 / funciones en 166.
Inversa, función 169 / operación 31-32 / transformación 285.
Inversión 227.
Inversos, elementos 31.
Irracionales, números 42, 44, 49.
Irreductible, polinomios 145-148, 188.
Isoclinostato 307.
Isomorfismo de orden 34.

K

Kempe, trisector de ángulo 307.
Klein, definición de una geometría 279.

L

Laplace, desarrollo de 254.
Lebesgue, teorema 55.
Limitados, números 53-54.
Límite 156, 158-163 / de sucesión 159 / de una raíz 206, 211.
Línea de una matriz 239.
Lineal, combinación 249 / congruencia 127-133 / consistente, sistema de ecuaciones 262 / dependencia 269-270 / ecuación, sistema de 260-268 / ecuación homogénea 260 / ecuación, teorema fundamental 265 / independencia 270 / orden 30 / subespacio 315 / transformación birracional 193.

M

Maclaurin, trisectriz de 305.
Manto 319.
Matriz 223 / ampliada 264 / aplicaciones geométricas 275-286 / características de 257-258 / coeficiente 264 / cofactores 240-241 / cuadrada 223/ cuadrada, determinan-

te 224 / cuadrada, diagonal principal 224 / cuadrada, orden de 224 / forma normal de 259 / iguales 281 / línea de una 239 / menor de una 240, 252-259 / notación de una 223, 224 / producto de una 255 / triangular 250.
Mayor divisor común 87, 100, 102, 141, 149, 208.
Media proporcional 294.
Menor complementario 253 / complemento algebraico de 253-254 / común múltiplo 87, 100, 142 / de un elemento 240 / principal 259 / r-ésimo 252.
Mersenne, primos de 96.
Método de los cuadrados menores 347 / de Horner 218-219 / de Newton 217-218.
Módulo de una congruencia 116-130 / de un número complejo 66 / recíproco 128-129.
Monomio 135-136.
Multiplicación conmutativa 28 / propiedades de la 24-28 / rusa campesina 110, 112.
Multiplicidad de raíces 212 / de intersecciones gráficas 317.

N

N-dimensional 314.
Natural, número 14 / orden 226.
Newton, diagrama 338-339 / método 217-218.
Nim 110.
Nodales, curvas 329.
Nodo 328.
Norma 66.
Notación decimal 113-115 / de los determinantes 223-225 / exponencial 27 / indo-arábiga 109 / de una matriz 223, 224.
Nueves, calcular 119.
Número 85-133 / algebraico 45 / amplitud de los 69-70 / argumento de los 69-70 / cardinales 14-20 / cardinales del continuo 60 / cardinales transfinitos 56-60 / clasificación 78 / complejos 63-78 / complejos, raíces imaginarias de 187-188 / compuestos 91 / constructibles 296 / cuociente de 66-67 / finitos 41 / ilimitados 53 / imaginarios 64 / irracionales 42, 44, 49 / limitados 53-54 / natural 14 / negativos 37-41 / no negativos 36 / ordinales 14 / parte imaginaria 64 / parte real 64 / perfectos 88 / primos 91-100 / racionales 33-41, 113-115 / reales 42, 44-46, 50, 55-56 / representación exponencial 69 / representación trigonométrica 69 / con signo 39 / sistemas de 13, 60-62, 79-82 / trascendente 45 / valor absoluto 39, 66 / valor numérico 39.

O

Operaciones binarias 18-19 / definidas 19 / inversas 31-32 / racionales 18.
Orden de un determinante 236 / de los elementos de un grupo cíclico 76 / isomorfismo de 34 / lineal 30 / de una matriz cuadrada 224, 236 / relaciones de (V. Relaciones de orden).
Ordenado, producto 282.
Ordinales, números 14.
Origen, tangente en el 338.
Oscilante, discontinuidad 167.

P

Pantógrafo 309.
Parábola 320 / semicúbica 328.
Paraboloide cúbico 328 / elíptico 324.
Parte imaginaria de los números 64 / real de un número 64.
Peano, postulado de 22-23.
Pendiente 171.
Permanencia 203, 227.
Permutación 225 / clases 227 / finita 229 / impar 227 / par 227.
Pitágoras, teorema 131.
Pitagórica, ecuación 131-133.
Plana, figura 297.
Plano complejo 66 / n-dimensional 314.
Polígonos articulados 306-310.
Polinomias, ecuaciones 177-220

Polinomios 135-176, 188-196, 208, 314-330 / anillo de 137-138 / asociados 141-142 / ceros de 178 / derivados de 170-172 / elementales simétricos 186, 188-195 / grado de 136-137 / gráficos de 314-329 / homogéneos 240, 338 / independientes 142 / irreductibles 145-148, 188 / primitivos 141 / primos entre sí 141 / reales 205 / reducibles 145 / simétricos 194-196 / de Sturm 208.
Postulado de Arquímides 89, 148 / de Dedekind 47 / de los números reales 46-50.
Potenciación 32.
Primitivas, raíces 76-77, 121-123 / soluciones 132.
Primos, números 91-101 / entre sí 87, 122, 141 / de Mersenne 96.
Principal, ideal 154 / menor, 259 / valor 70-74.
Principio de inducción completa 23.
Problema de Delos 300 / diofánticos 131-133.
Producto interno 255 / de matrices 255-256 / ordenado 282 / símbolo de 99.
Promedio aritmético 37 / geométrico 291, 294.
Pruebas para la divisibilidad 118-120, 179.
Punto aislado 328 / de círculo 318-319 / entero 51 / doble 328 / ramificación 335 / reflexión de un 285 / singular 327.

R

Racionales, funciones 139, 329-333 / números 33-41, 113-114 / operaciones 18 / raíces 194.
Raíces, acotación de 206, 210-211 / aislar 211 / conjugadas imaginarias 187 / construcción de 296-298 / de ecuación 177, 183-185, 191-196, 211, 212-216 / extracción de 32 / imaginarias de los números complejos 187-188 / límite de 206, 211 / multiplicidad de 212 / múltiples, teorema de Sturm 214 / primitivas 76-77, 121, 123 / racionales 194 / simples 212 / transformaciones de 191-196 / de la unidad 76, 121-123.
Ramificación, puntos de 335.
Rango de una función 155.
Real, gráfico 334.
Reales, ecuaciones 205 / números 42, 44, 46-50, 55-56.
Recíproco, módulo 128-129.
Reducida, ecuación cúbica 198.
Reducible, curva 341 / polinomio 145.
Reducción al absurdo 42.
Reflexión de un punto 285.
Región excluida 337.
Regla 289 / de Cramer 222, 260-263 / de los signos de Descartes 202-207.
Relaciones binarias 19 /de equivalencia 20-21 / de identidad 140, 177 / de orden de enteros no negativos 29-31, 33 / de orden de números cardinales 56 / de orden de números complejos 17 / de orden de números racionales 34-42 / de orden de números reales 46-51 / reflexiva 20 / simétrica 20-21.
Representación exponencial de los números 69 / trigonométrica de los números 69.
Residuales, clases 120-123, 153.
Residuo módulo 120 / sistema completo 121 / sistema reducido 122-123.
R-ésimo, menor 252.
Resolvente cúbica 201-202.
Resto, teorema del 130, 178.
Riemann, superficie de 334-335.
Rotación 280.

S

Secante 171.
Segmento 155.
Serie infinita 162-174 / de Taylor 173-176.
Símbolo de la suma 236.
Simétricas, funciones 195-196 / gráficos 337 / polinomios

194-196 / relaciones 20-21.
Sintética, división 179-182, 206.
Sistemas de ecuaciones lineales 260-268.
Soluciones 33, 128, 131, 132, 177 / aproximadas 217-220 / gráficas 343-345.
Sturm, funciones de 208 / polinomios de 208 / sucesiones 208, 213-214 / teorema de 207-213 / teorema para raíces múltiples 214.
Subconjunto 16-17.
Subespacio lineal 315.
Sucesión 158 / de Cauchy 55, 160, 176 / convergente 160 / división 208 / infinita 162, 174 / límite de 159 / nula 159 / de Sturm 208, 213-216.
Suma, símbolo de 236.
Superficies cuádricas 323 / reglada 325-326 / de Riemann 334-335.
Sustracción 32.

T

Tangentes 171 / en el origen 338.
Taylor, fórmula de 173 / serie de 173-176.
Teorema de Bolzano-Weierstrass 55 / de Cantor-Dedekind 52, 55 / chino del resto 130 / de Dedekind 47 / de De Moivre 74-79 / de Euler 126 / del factor 178 / de la factorización única 98 / de Fermat, simple 126-127 / de Fermat, último 131-133 / fundamental del álgebra 184 / fundamental de la aritmética 98 / fundamental para sistemas de ecuaciones lineales 265 / de Heine-Bφrel-Lebesgue 55 / de Pitágoras 131 / del resto 178 / de Sturm 207-213 / de Wilson 131.
Teoría de las ecuaciones 177-220 / de los números 85-133.
Tetradimensional, espacio 325-327.
Tomahawk 306.
Totient de m 122.
Transfinito, número cardinal 56.
Transformaciones, afín 283 / elementales 259 / de Euclides 284 / geométricas 279-286 / grupo de 285 / homotéticas 286 / de identidad 285 / inversas 285 / lineal birracional 193 / producto ordenado de las 282 / de raíces 191-196.
Transitividad 20-21.
Transposiciones 229-234.
Trascendente, función 175-176 / número 45.
Traslación 279-280.
Trazado de curvas 308, 336-343.
Triangular, matriz 250.
Trinomio 136.
Trigonométrica, representación de los números 69.
Trisección de un ángulo, clásica 301, 302 / no clásica 303-308 / de Arquímides 304 / de Kempe 307.
Trisectriz de Maclaurin 305.

U

Uniersal, curva 329.
Unidad 26, 27, 87 / raíces de la 76-77, 121-123.
Unidades 87, 91, 141.
Uniforme, función 155.
Uno a uno, correspondencia 14.

V

Vacío, conjunto 17, 47 / gráfico 314.
Valor absoluto 39, 66 / principal 70-74.
Vandermonde, determinante 251-252.
Variable, 127-128, 135 / cambio de 151-153, 181-183 / dependiente 154 / entera positiva 155 / independiente 154 / real continua 155.
Variación 202-203.
Vector 69.
Vertical, asíntota 330.

W

Weierstrass, teorema de 55.
Wilson, teorema de 131.

Símbolos y Notación

Los símbolos y notación siguientes aparecen por primera vez y se definen en las páginas que se indican a la izquierda.

PAGINA		PAGINA	
16, 19	$=$	137	$p(x)$
16, 29	$<$	154	$f(x)$
16, 29	$>$	157	$[x]$
21	$\neq$	158	$\{a_n\}$
23	a^+	159	ε
33, 34	a/b		N_ε
37	$[a - b]$	159	$\lim_{n\to\infty} a_n$
39	$\|c\|$		
47	$\{L, R\}$	162	$\sum_{n=1}^{\infty} a_n$
57	$\aleph_0$	163	$n = 1$
64	(a, b)	165	$\lim_{x\to a^-} f(x)$
66	$n(z)$		
	$\|z\|$	165	$\lim_{x\to a^+} f(x)$
80	$R[k]$		
	$R(k)$	168	δ_{ij}
82	$R^*(i)$	170	$p'(x)$
86	$b\|a$	172	$p^{(m)}(x)$
87	(a, b)	210	S_n
87	$[a, b]$	224	$[a_{ij}]$, $i, j = 1, 2, \ldots, n$
95	$b + a$	224	$\|a_{ij}\|$, $i, j = 1, 2, \ldots, n$
99	$\amalg$	225	P_n
107	334_6	229	(ab)
116	$a \equiv b \pmod m$	236	Σ
121	$a \not\equiv b \pmod m$	253	C_{n-r}^{n}
121	$[r] \pmod m$	339	f_n
122	$\phi(m)$		